Samba-HOWTO-Sammlung

Jelmer R. Vernooij, John H. Terpstra, Gerald (Jerry) Carter und German Translation

1. Oktober 2004

Zusammenfassung

Dieses Buch ist eine Sammlung von HOWTOs, welche über die Jahre hinweg der Samba-Dokumentation hinzugefügt wurden. Samba ist immer unter Weiterentwicklung und so auch die Dokumentation dazu. Diese Veröffentlichung der Dokumentation stellt eine große Veränderung der Dokumentation bzw. des Layouts dar. Die aktuelle Version dieser Dokumentation (englisch) finden Sie unter <`http://www.samba.org/`> auf der "DocumentationSSeite. Bitte senden Sie Neuigkeiten an Jelmer Vernooij <`mailto:jelmer@samba.org`>, John H. Terpstra <`mailto:jht@samba.org`> oder Gerald (Jerry) Carter <`mailto:jerry@samba.org`>.

Anmerkungen zur deutschen Fassung senden Sie bitte an Stefan G. Weichinger <`mailto:monitor@oops.co.at`>.

Das Samba-Team möchte den vielen Personen seinen aufrichtigen Dank ausdrücken, die durch ihr Wissen oder Unwissen zu diesem Update der Doku beigetragen haben. Die Größe und der Umfang dieses Projekts hätten ohne die wichtigen Beiträge der Community niemals solche Ausmaße angenommen. Eine nicht bedeutungslose Anzahl von Ideen kamen aus einer Anzahl von inoffiziellen HOWTOs - an jeden Autor dieser HOWTOs auch ein recht herzliches Dankeschön. Bitte macht weiter mit der Veröffentlichung eurer inoffiziellen HOWTOs - sie sind eine Quelle der Inspiration und des Erfahrungs-Austauschs von vielen Samba-Benutzern und -Administratoren.

COPYRIGHT INFORMATIONEN

Diese Dokumentation wird unter der GNU General Public License (GPL) Version 2 veröffentlicht. Eine Kopie dieser Lizenzbestimmung ist in den Samba-Quelldateien enthalten und kann ebenfalls unter <`http://www.fsf.org/licenses/gpl.txt`> eingesehen werden.

ZUSCHREIBUNG

Einführung in Samba

- David Lechnyr <david@lechnyr.com <mailto:david@lechnyr.com>>
- Hendrik Bäcker <h_baecker@gmx.net <mailto:h_baecker@gmx.net>> (Deutsche Übersetzung)

Wie man Samba installiert und testet

- Andrew Tridgell <tridge@samba.org <mailto:tridge@samba.org>>
- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Karl Auer <kauer@biplane.com.au <mailto:kauer@biplane.com.au>>
- Dan Shearer <dan@samba.org <mailto:dan@samba.org>>
- Hendrik Bäcker <h_baecker@gmx.net <mailto:h_baecker@gmx.net>> (Deutsche Übersetzung)

Schnellstart: Allheilmittel für Ungeduldige

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Joachim Luft <joachim@luft-it.de <mailto:joachim@luft-it.de>> (Deutsche Übersetzung)

Server-Arten und Sicherheitsmodi

- Andrew Tridgell <tridge@samba.org <mailto:tridge@samba.org>>
- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Hendrik Bäcker <h_baecker@gmx.net <mailto:h_baecker@gmx.net>> (Deutsche Übersetzung)

Die Kontrolle über eine Domäne

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Gerald (Jerry) Carter <jerry@samba.org <mailto:jerry@samba.org>>
- David Bannon <dbannon@samba.org <mailto:dbannon@samba.org>>
- Günther Deschner <gd@suse.de <mailto:gd@suse.de>> (LDAP updates)
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Backup Domänen-Verwaltung

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Volker Lendecke <Volker.Lendecke@SerNet.DE <mailto:Volker.Lendecke@SerNet.DE>>
- Günther Deschner <gd@suse.de <mailto:gd@suse.de>> (LDAP updates)
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Domänen-Mitgliedschaft

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Jeremy Allison <jra@samba.org <mailto:jra@samba.org>>
- Gerald (Jerry) Carter <jerry@samba.org <mailto:jerry@samba.org>>
- Andrew Tridgell <tridge@samba.org <mailto:tridge@samba.org>>
- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- Günther Deschner <gd@suse.de <mailto:gd@suse.de>> (LDAP updates)
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Stand-alone-Server

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Anleitung zur MS Windows Netzwerkkonfiguration

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Joachim Luft <joachim@luft-it.de <mailto:joachim@luft-it.de>> (Deutsche Übersetzung)

Netzwerk-Browsing

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Die Account-Datenbank

- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Gerald (Jerry) Carter <jerry@samba.org <mailto:jerry@samba.org>>
- Jeremy Allison <jra@samba.org <mailto:jra@samba.org>>

- Günther Deschner <gd@suse.de <mailto:gd@suse.de>> (LDAP updates)
- Olivier (lem) Lemaire <olem@IDEALX.org <mailto:olem@IDEALX.org>>
- Rainer Dölker <rainer.doelker@hp.com <mailto:rainer.doelker@hp.com>> (Deutsche Übersetzung)
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Das Gruppen-Mapping zwischen MS Windows und UNIX

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Jean François Micouleau
- Gerald (Jerry) Carter <jerry@samba.org <mailto:jerry@samba.org>>
- Joachim Luft <joachim@luft-it.de <mailto:joachim@luft-it.de>> (Deutsche Übersetzung)

Zugriffskontrollen für Dateien, Verzeichnisse und Netzwerk-Freigaben

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Jeremy Allison <jra@samba.org <mailto:jra@samba.org>>
- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>> (drawing)
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Joachim Luft <joachim@luft-it.de <mailto:joachim@luft-it.de>> (Deutsche Übersetzung)

Datei- und Satzsperren

- Jeremy Allison <jra@samba.org <mailto:jra@samba.org>>
- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Eric Roseme <eric.roseme@hp.com <mailto:eric.roseme@hp.com>>
- Joachim Luft <joachim@luft-it.de <mailto:joachim@luft-it.de>> (Deutsche Übersetzung)

Samba absichern

- Andrew Tridgell <tridge@samba.org <mailto:tridge@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Interdomain Vertrauensstellungen

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Rafal Szczesniak <mimir@samba.org <mailto:mimir@samba.org>>

- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>> (drawing)
- Stephen Langasek <vorlon@netexpress.net <mailto:vorlon@netexpress.net>>
- Felix Erlacher <erlacher@virgilio.it <mailto:erlacher@virgilio.it>> (Deutsche Übersetzung)

Betreiben eines Microsoft Distributed File System Baumes

- Shirish Kalele <samba@samba.org <mailto:samba@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Felix Erlacher <erlacher@virgilio.it <mailto:erlacher@virgilio.it>> (Deutsche Übersetzung)
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Klassische Druckerunterstützung

- Kurt Pfeifle <kpfeifle@danka.de <mailto:kpfeifle@danka.de>>
- Gerald (Jerry) Carter <jerry@samba.org <mailto:jerry@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Dinu Gherman <gherman@darwin.in-berlin.de <mailto:gherman@darwin.in-berlin.de>> (Deutsche Übersetzung)

Unterstützung des CUPS-Drucksystems

- Kurt Pfeifle <kpfeifle@danka.de <mailto:kpfeifle@danka.de>>
- Ciprian Vizitiu <CVizitiu@gbif.org <mailto:CVizitiu@gbif.org>> (drawings)
- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>> (drawings)
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Stapelbare VFS Module

- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Tim Potter <tpot@samba.org <mailto:tpot@samba.org>>
- Simo Sorce (original vfs_skel README)
- Alexander Bokovoy (original vfs_netatalk docs)
- Stefan Metzmacher (Update for multiple modules)
- Felix Erlacher <erlacher@virgilio.it <mailto:erlacher@virgilio.it>> (Deutsche Übersetzung)

Winbind: Benutzung von Domänenkonten

- Tim Potter <tpot@linuxcare.com.au <mailto:tpot@linuxcare.com.au>>

- Andrew Tridgell <tridge@samba.org <mailto:tridge@samba.org>>
- Naag Mummaneni <getnag@rediffmail.com <mailto:getnag@rediffmail.com>> (Notes for Solaris)
- John Trostel <jtrostel@snapserver.com <mailto:jtrostel@snapserver.com>>
- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Fortgeschrittenes Netzwerk-Management

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

System und Zugriffs-Richtlinien

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Joachim Luft <joachim@luft-it.de <mailto:joachim@luft-it.de>> (Deutsche Übersetzung)

Das Management von Desktop-Profilen

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

PAM-basierte verteilte Authentifizierung

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Stephen Langasek <vorlon@netexpress.net <mailto:vorlon@netexpress.net>>
- Felix Erlacher <erlacher@virgilio.it <mailto:erlacher@virgilio.it>> (Deutsche Übersetzung)

Samba in MS-Windows-Netzwerke integrieren

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Thomas Reiss <thomas@mypoint.franken.de <mailto:thomas@mypoint.franken.de>> (Deutsche Übersetzung)

Unicode/Zeichensätze

- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Takahashi Motonobu <monyo@home.monyo.com <mailto:monyo@home.monyo.com>> (Japanese character support)

- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Backup-Techniken

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Hochverfügbarkeit

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Jeremy Allison <jra@samba.org <mailto:jra@samba.org>>
- Joachim Luft <joachim@luft-it.de <mailto:joachim@luft-it.de>> (Deutsche Übersetzung)

Upgrade von Samba-2.x auf Samba-3.0.0

- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Gerald (Jerry) Carter <jerry@samba.org <mailto:jerry@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Migration von einem NT4-PDC auf einen Samba-3-PDC

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

SWAT Das Samba-Administrations-Werkzeug

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Markus Klimke <m.klimke@tu-harburg.de <mailto:m.klimke@tu-harburg.de>> (Deutsche Übersetzung)

Die Samba Checkliste

- Andrew Tridgell <tridge@samba.org <mailto:tridge@samba.org>>
- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- Dan Shearer <dan@samba.org <mailto:dan@samba.org>>
- Thomas Reiss <thomas@mypoint.franken.de <mailto:thomas@mypoint.franken.de>> (Deutsche Übersetzung)

Analyse und Lösung von Problemen mit Samba

- Gerald (Jerry) Carter <jerry@samba.org <mailto:jerry@samba.org>>
- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>

- David Bannon <dbannon@samba.org <mailto:dbannon@samba.org>>
- Dan Shearer <dan@samba.org <mailto:dan@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Das Melden von Fehlern

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- Andrew Tridgell <tridge@samba.org <mailto:tridge@samba.org>>
- Hendrik Bäcker <h_baecker@gmx.net <mailto:h_baecker@gmx.net>> (Deutsche Übersetzung)

Wie man Samba kompiliert

- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Andrew Tridgell <tridge@samba.org <mailto:tridge@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Portabilität

- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Samba und andere CIFS-Clients

- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Dan Shearer <dan@samba.org <mailto:dan@samba.org>>
- Jim McDonough <jmcd@us.ibm.com <mailto:jmcd@us.ibm.com>> (OS/2)
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Samba Performance Tuning

- Paul Cochrane <paulc@dth.scot.nhs.uk <mailto:paulc@dth.scot.nhs.uk>>
- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

DNS und DHCP: Konfigurations-Anleitung

- John H. Terpstra <jht@samba.org <mailto:jht@samba.org>>
- Stefan G. Weichinger <monitor@oops.co.at <mailto:monitor@oops.co.at>> (Deutsche Übersetzung)

Weitere Hilfsquellen.

- Jelmer R. Vernooij <jelmer@samba.org <mailto:jelmer@samba.org>>
- Hendrik Bäcker <h_baecker@gmx.net <mailto:h_baecker@gmx.net>> (Deutsche Übersetzung)

CONTENTS

Contents

COPYRIGHT INFORMATIONEN v

ZUSCHREIBUNG vi

Part I Grundlegende Installation xxxi

VORBEREITUNG ZUR SAMBA-KONFIGURATION 1

Chapter 1 EINFÜHRUNG IN SAMBA 2
1.1 Hintergrund 2
1.2 Fachsprache 3
1.3 Verwandte Projekte 4
1.4 SMB-Methodologie 4
1.5 Epilog 5

Chapter 2 WIE MAN SAMBA INSTALLIERT UND TESTET 7
2.1 Wie man Samba bekommt und installiert 7
2.2 Samba konfigurieren (smb.conf) 7
2.2.1 Die Syntax der Konfiguration 7
2.2.2 Samba starten 8
2.2.3 Beispielkonfiguration 8
2.2.3.1 Test der Konfiguration mit testparm 9
2.2.4 SWAT 9
2.3 Auflistung von Freigaben auf dem Server 10
2.4 Verbindung zu einem UNIX-Client aufbauen 10
2.5 Verbindung von einem entfernten SMB-Client 11
2.6 Was tun, wenn etwas nicht funktioniert? 11
2.7 Häufige Fehler 11
2.7.1 Große Anzahl von smbd-Prozessen 11
2.7.2 Fehlermeldung: open_oplock_ipc 12
2.7.3 Fehlermeldung:„*The network name cannot be found*“ 12

Chapter 3 SCHNELLSTART: ALLHEILMITTEL FÜR UNGEDULDIGE 13
3.1 Eigenschaften und Vorzüge 13
3.2 Beschreibung von Beispielseiten 13
3.3 Arbeitsbeispiele 14
3.3.1 Stand-alone-Server 14
3.3.1.1 Anonymer Nur-Lese-Dokumenten-Server 14
3.3.1.2 Anonymer Schreib-Lese-Dokumenten-Server 16
3.3.1.3 Anonymer Druckserver 17

3.3.1.4 Sicherer Lese-Schreib-Datei- und Druck-Server 19
3.3.2 Domänen-Mitgliedsserver 22
3.3.2.1 Beispielkonfiguration 23
3.3.3 Domänencontroller 26
3.3.3.1 Beispiel: Ingenieur-Büro 27
3.3.3.2 Eine große Organisation 28

Part II Basiswissen zur Server-Konfiguration 33

ERSTE SCHRITTE BEI DER KONFIGURATION 35

Chapter 4 SERVER-ARTEN UND SICHERHEITSMODI 36
4.1 Positive Merkmale und Vorteile 36
4.2 Server-Arten 37
4.3 Samba-Sicherheitsmodi 37
4.3.1 User Level-Sicherheit 38
4.3.1.1 Beispielkonfiguration 38
4.3.2 Share Level-Sicherheit 38
4.3.2.1 Beispielkonfiguration 39
4.3.3 Domänen-Sicherheitsmodus (User Level Security) 39
4.3.3.1 Beispielkonfiguration 39
4.3.4 ADS-Sicherheitsmodus (User Level Security) 40
4.3.4.1 Beispielkonfiguration 41
4.3.5 Server Security (User Level Security) 41
4.3.5.1 Beispielkonfiguration 42
4.4 Passwort-Prüfung 42
4.5 Häufige Fehler 44
4.5.1 Was macht Samba zu einem Server? 44
4.5.2 Was macht Samba zu einem Domänencontroller? 44
4.5.3 Was macht Samba zu einem Domänen-Mitglied? 44
4.5.4 Verlieren der Verbindung zum Passwort-Server 44

Chapter 5 DIE KONTROLLE ÜBER EINE DOMÄNE 45
5.1 Eigenschaften und Vorzüge 46
5.2 Grundlagen der Domänen-Verwaltung 48
5.2.1 Typen von Domänencontrollern 48
5.2.2 Vorbereitungen für die Domänen-Verwaltung 50
5.3 Domänen-Verwaltung — Beispielkonfiguration 52
5.4 ADS-Domänen-Verwaltung mit Samba 54
5.5 Konfiguration der Domänen- und Netzwerk-Anmeldung 55
5.5.1 Domänen-Netzwerks-Anmelde-Dienst 55
5.5.1.1 Beispiel für eine Konfiguration 55
5.5.1.2 Der spezielle Fall von MS Windows XP Home Edition 55
5.5.1.3 Der spezielle Fall von Windows 9x/Me 56
5.5.2 Sicherheitsmodus und Master Browser 57
5.6 Häufige Fehler 58
5.6.1 „$“ darf nicht im Maschinen-Namen vorkommen 58

5.6.2 Der Anschluss an die Domäne scheitert an einem bereits existierenden Maschinen-Konto 59
5.6.3 Das System kann Sie nicht anmelden (C000019B) 59
5.6.4 Das Maschinen-Vertrauenskonto ist nicht erreichbar 60
5.6.5 Konto deaktiviert 60
5.6.6 Domänencontroller nicht verfügbar 60
5.6.7 Ich kann mich nicht an einer Domänen-Mitglieds-Workstation anmelden, nachdem ich mich einer Domäne angeschlossen habe 61

Chapter 6 BACKUP-DOMÄNEN-VERWALTUNG 62
6.1 Eigenschaften und Vorzüge 62
6.2 Essenzielle Hintergrund-Informationen 63
6.2.1 Domänen-Verwaltung im Stil von MS Windows NT4 64
6.2.1.1 Beispiel einer PDC-Konfiguration 65
6.2.2 Bemerkungen zur LDAP-Konfiguration 66
6.2.3 Domänen-Verwaltung mit Active-Directory 67
6.2.4 Was zeichnet einen Domänencontroller im Netzwerk aus? 67
6.2.5 Wie findet eine Workstation ihren Domänencontroller? 67
6.2.5.1 NetBIOS über TCP/IP aktiviert 67
6.2.5.2 NetBIOS über TCP/IP deaktiviert 68
6.3 Konfiguration eines Backup-Domänen-Controllers 68
6.3.1 Beispielkonfiguration 69
6.4 Häufige Fehler 70
6.4.1 Maschinen-Konten laufen immer wieder ab 70
6.4.2 Kann Samba ein BDC für einen NT4-PDC sein? 70
6.4.3 Wie repliziere ich die Datei smbpasswd? 70
6.4.4 Kann ich all dies mit LDAP erledigen? 71

Chapter 7 DOMÄNEN-MITGLIEDSCHAFT 72
7.1 Eigenschaften und Vorzüge 72
7.2 Maschinen-Vertrauenskonten mit MS Windows Workstations bzw. Servern 73
7.2.1 Manuelles Anlegen von Maschinen-Vertrauenskonten 74
7.2.2 Das Verwalten von Domänen-Maschinen-Konten mit dem Server Manager 75
7.2.3 „*On-the-Fly*“-Anlegen von Maschinen-Konten 76
7.2.4 Eine MS Windows-Workstation oder einen MS Windows-Server zum Domänen-Mitglied machen 76
7.2.4.1 Windows 200x/XP Professional-Client 76
7.2.4.2 Windows NT4-Client 77
7.2.4.3 Samba-Client 77
7.3 Domänen-Mitgliedsserver 77
7.3.1 Sich mit Samba-3 einer NT4-Domäne anschließen 78
7.3.2 Warum ist dies besser als security = server? 80
7.4 Samba-ADS-Domänen-Mitgliedschaft 81
7.4.1 Das Konfigurieren von smb.conf 81
7.4.2 Das Konfigurieren von /etc/krb5.conf 81
7.4.3 Anlegen des Maschinen-Kontos 83
7.4.3.1 Mögliche Fehler 85

7.4.4 Testen des Server-Setups 85
7.4.5 Testen mit smbclient 85
7.4.6 Bemerkungen 85
7.5 Gemeinsames Nutzen von UID-Zuweisungen unter Samba-Domänen-Mitgliedern 86
7.6 Gängige Fehler 86
7.6.1 Eine Maschine kann nicht noch einmal der Domäne hinzugefügt werden 86
7.6.2 Das Hinzufügen einer Maschine zur Domäne scheitert 87
7.6.3 Ich kann mich keinem Windows 2003-PDC anschließen 87

Chapter 8 STAND-ALONE-SERVER 88
8.1 Eigenschaften und Vorzüge 88
8.2 Hintergrund 88
8.3 Beispiel-Konfiguration 89
8.3.1 Referenz-Dokumentationsserver 89
8.3.2 Zentrales Druck-Serving 89
8.4 Gängige Fehler 91

Chapter 9 ANLEITUNG ZUR MS WINDOWS NETZWERKKONFIGURATION 92
9.1 Eigenschaften und Vorzüge 92
9.2 Technische Details 92
9.2.1 TCP/IP Konfiguration 92
9.2.1.1 MS Windows XP Professional 93
9.2.1.2 MS Windows 2000 95
9.2.1.3 MS Windows Me 98
9.2.2 Einer Domäne beitreten: Windows 2000/XP Professional 101
9.2.3 Konfiguration der Domänen-Anmeldung: Windows 9x/Me 103
9.3 Allgemeine Fehler 106

Part III Erweiterte Konfiguration 107

WERTVOLLE INFORMATIONEN 109

Chapter 10 NETZWERK-BROWSING 110
10.1 Planung und Beginn 110
10.2 Was ist Browsing? 111
10.3 Diskussion 112
10.3.1 NetBIOS-über-TCP/IP 112
10.3.2 TCP/IP ohne NetBIOS 113
10.3.3 DNS und Active Directory 114
10.4 Wie Browsing funktioniert 116
10.4.1 Konfiguration des ARBEITSGRUPPEN-Browsings 117
10.4.2 Konfiguration des DOMÄNEN-Browsings 118
10.4.3 Wie man Samba dazu zwingt, der Master zu sein 119
10.4.4 Wie man Samba zum Domänen-Master macht 120
10.4.5 Bemerkung zu Broadcast-Adressen 121
10.4.6 Mehrere Interfaces 121
10.4.7 Verwendung des Parameters Remote Announce 121

10.4.8 Verwendung des Parameters Remote Browse Sync 121
10.5 WINS — Der „*Windows Internetworking Name Server*“ 122
10.5.1 Die Konfiguration des WINS-Servers 123
10.5.2 WINS-Replikation 124
10.5.3 Statische WINS-Einträge 124
10.6 Hilfreiche Hinweise 125
10.6.1 Windows-Netzwerk-Protokolle 125
10.6.2 Die Reihenfolge der Namensauflösung 126
10.7 Technischer Überblick über das Browsing 126
10.7.1 Die Unterstützung des Browsings in Samba 127
10.7.2 Problemlösung 127
10.7.3 Cross-Subnetz-Browsing 128
10.7.3.1 Das Verhalten des Cross-Subnetz-Browsings 128
10.8.4 Wichtige Bemerkungen zur Sicherheit 133
10.8.4.1 Vorteile verschlüsselter Passwörter 134
10.8.4.2 Vorteile nichtverschlüsselter Passwörter 135
10.8.5 Die Zuordnung von Benutzer-Identifiern (UIDs) zwischen MS Windows und UNIX 135
10.8.6 Das Zuweisen gemeinsamer UIDs/GIDs auf verteilten Maschinen 135
10.9 Werkzeuge zur Verwaltung von Konten 136
10.9.1 Der Befehl *smbpasswd* 136
10.9.2 Der Befehl *pdbedit* 137
10.10 Passwort-Backends 139
10.10.1 Klartext 139
10.10.2 smbpasswd — Datenbank für verschlüsselte Passwörter 139
10.10.3 tdbsam 140
10.10.4 ldapsam 140
10.10.4.1 Unterstützte LDAP-Server 141
10.10.4.2 Schema und Verhältnis zum RFC 2307-posixAccount 141
10.10.4.3 OpenLDAP-Konfiguration 142
10.10.4.4 Das Initialisieren der LDAP-Datenbank 143
10.10.4.5 Die Konfiguration von Samba 145
10.10.4.6 Das Management von Benutzern und Gruppen 145
10.10.4.7 Sicherheit und sambaSamAccount 146
10.10.4.8 Spezielle LDAP-Attribute für sambaSamAccounts 147
10.10.4.9 Beispiel für LDIF-Einträge eines sambaSamAccount 147
10.10.4.10 Die Synchronisation von Passwörtern 148
10.10.5 MySQL 149
10.10.5.1 Das Anlegen der Datenbank 149
10.10.5.2 Konfigurieren 149
10.10.5.3 Klartext-Passwörter oder verschlüsselte Passwörter 150
10.10.5.4 Das Beziehen von Nicht-Spalten-Daten aus der Tabelle 151
10.10.6 XML 151
10.11 Gängige Fehler 151
10.11.1 Benutzer können sich nicht anmelden 151
10.11.2 Benutzer werden zur falschen Backend-Datenbank hinzugefügt 151
10.11.3 Konfiguration der auth methods 152

Chapter 11 DAS GRUPPEN-MAPPING — ZWISCHEN MS WINDOWS UND UNIX 156
11.1 Eigenschaften und Vorzüge 156
11.2 Diskussion 157
11.2.1 Wichtige administrative Informationen 159
11.2.2 Standardbezeichner für Benutzer, Gruppen und Beziehungen 159
11.2.3 Beispielkonfiguration 160
11.3 Konfigurationskripten 161
11.3.1 Beispiel für ein smb.conf-Skript zum Hinzufügen von Gruppen 161
11.3.2 Skript zum Konfigurieren von Gruppen-Mappings 161
11.4 Gängige Fehler 162
11.4.1 Das Hinzufügen von Gruppen schlägt fehl 162
11.4.2 Das Hinzufügen von MS Windows-Gruppen zu MS Windows-Gruppen schlägt fehl 163
11.4.3 *Domänen Benutzer* zu der Gruppe *Hauptbenutzer* hinzufügen 163

Chapter 12 ZUGRIFFSKONTROLLEN FÜR DATEIEN, VERZEICHNISSE UND NETZWERK-FREIGABEN 164
12.1 Möglichkeiten und Vorteile 164
12.2 Die Zugriffskontrollen des Dateisystems 165
12.2.1 Vergleich zwischen NTFS und dem UNIX-Dateisystem 165
12.2.2 Verwaltung von Verzeichnissen 167
12.2.3 Die Verwaltung der Zugriffskontrollen von Dateien und Ordnern (Verzeichnissen) 167
12.3 Zugriffskontrollen für Freigabedefinitionen 169
12.3.1 Benutzer- und gruppen-basierende Kontrollen 169
12.3.2 Kontrollen, die auf Datei- und Verzeichnis-Berechtigungen basieren 169
12.3.3 Allgemeine Kontrollen 170
12.4 Zugriffskontrollen auf Freigaben 171
12.4.1 Verwaltung von Freigabeberechtigungen 172
12.4.1.1 Windows NT4 Workstation/Server 172
12.4.1.2 Windows 200x/XP 173
12.5 MS Windows-Zugriffskontroll-Listen (ACLs) und UNIX-Wechselwirkungen 174
12.5.1 Verwalten von UNIX-Berechtigungen durch NT-Sicherheitsdialoge 174
12.5.2 Anzeigen von Dateisicherheit auf einer Samba-Freigabe 174
12.5.3 Anzeigen von Dateieigentümern 175
12.5.4 Das Anzeigen von Datei- oder Verzeichnisberechtigungen 175
12.5.4.1 Dateiberechtigungen 176
12.5.4.2 Verzeichnis-Berechtigungen 176
12.5.5 Ändern von Datei- oder Verzeichnis-Berechtigungen 177
12.5.6 Die Wechselwirkung mit den Samba-Standard-Parametern „*create mask*“ 177
12.5.7 Die Wechselwirkung mit den Standard-Samba-Dateiattribut-Vergaben 179
12.6 Gängige Fehler 179
12.6.1 Benutzer können nicht auf eine öffentliche Freigabe schreiben 179
12.6.2 Dateioperationen, die als *root* mit *force user* ausgeführt wurden 181
12.6.3 MS Word mit Samba ändert den Eigentümer einer Datei 181

Chapter 13 DATEI- UND SATZSPERREN 184
13.1 Eigenschaften und Vorzüge 184
13.2 Erörterung 185
13.2.1 Überblick über opportunistische Sperren 185
13.2.1.1 Exklusive Freigaben 188
13.2.1.2 Freigaben oder Dateien, auf die von mehreren Usern zugegriffen wird 188
13.2.1.3 Dateien, auf die von UNIX- oder NFS-Clients aus zugegriffen wird 188
13.2.1.4 Langsame und/oder unzuverlässige Netzwerke 189
13.2.1.5 Mehrbenutzer-Datenbanken 189
13.2.1.6 PDM-Daten-Freigaben 189
13.2.1.7 Vorsicht vor Force User 189
13.2.1.8 Erweiterte Samba-Oplock-Parameter 190
13.2.1.9 Missionskritische Hochverfügbarkeit 190
13.3 Samba-Oplock-Kontrolle 191
13.3.1 Beispielkonfiguration 192
13.3.1.1 Oplocks deaktivieren 192
13.3.1.2 Kernel-Oplocks deaktivieren 192
13.4 Oplock- und Cache-Kontrollen mit MS Windows 194
13.4.1 Workstation-Dienst-Einträge 196
13.4.2 Server-Dienst-Einträge 196
13.5 Andauernder Datenverlust 197
13.6 Häufige Fehler 197
13.6.1 Fehlermeldungen bezüglich locking.tdb 198
13.6.2 Probleme beim Speichern von Dateien in MS Office auf Windows XP 198
13.6.3 Lange Verzögerungen beim Löschen von Dateien über das Netzwerk mit XP SP1 198
13.7 Weiterer Lesestoff 199

Chapter 14 SAMBA ABSICHERN 200
14.1 Einführung 200
14.2 Eigenschaften und Vorzüge 200
14.3 Technische Beschreibung von Schutzmaßnahmen 201
14.3.1 Host-basierter Schutz 201
14.3.2 Benutzer-basierter Schutz 201
14.3.3 Benutzen von Schnittstellen-Schutz 201
14.3.4 Verwendung einer Firewall 202
14.3.5 Verwenden von Ablehnungen, die auf IPC$-Freigaben basieren 202
14.3.6 NTLMv2-Sicherheit 203
14.4 Upgrade von Samba 203
14.5 Häufige Fehler 203
14.5.1 Smbclient funktioniert auf Localhost, aber das Netzwerk ist tot 204
14.5.2 Warum können Benutzer auf die home-Verzeichnisse anderer Benutzer zugreifen? 204

Chapter 15 INTERDOMAIN-VERTRAUENSSTELLUNGEN 205
15.1 Eigenschaften und Vorzüge 205

15.2 Hintergrund von Vertrauensstellungen 205
15.3 Native MS Windows NT4-Vertrauenstellungen konfigurieren 206
15.3.1 Eine NT4-Vertrauensstellung aufbauen 206
15.3.2 Eine NT4-Vertrauensstellung fertig stellen 207
15.3.3 Interdomain-Vertrauensmöglichkeiten 207
15.4 Konfigurieren einer NT-artigen Vertrauensstellung mit Samba 208
15.4.1 Samba als vertraute Domäne 208
15.4.2 Samba als die vertrauende Domäne 209
15.5 NT4-artie Domänen-Vertrauensstellungen mit Windows 2000 210
15.6 Häufige Fehler 210
15.6.1 Das Durchsuchen der vertrauten Domäne schlägt fehl 210
15.6.2 Probleme mit LDAP ldapsam und den smbldap-Tools 211

Chapter 16 BETREIBEN EINES MICROSOFT DISTRIBUTED-FILE-SYSTEM-BAUMS 213
16.1 Eigenschaften und Vorzüge 213
16.2 Gängige Fehler 214
16.2.1 Der MSDFS-UNIX-Pfad ist „*case-critical*“ 214

Chapter 17 KLASSISCHE DRUCKERUNTERSTÜTZUNG 216
17.1 Eigenschaften und Vorzüge 216
17.2 Technische Informationen 217
17.2.1 Übergabe eines Druckauftrags vom Client an Samba 218
17.2.2 Druckrelevante Konfigurationsparameter 218
17.3 Einfache Druckkonfiguration 218
17.3.1 Überprüfen der Konfiguration mit testparm 219
17.3.2 Schnelle Validierung der Konfiguration 220
17.4 Erweiterte Druckerkonfiguration 223
17.4.1 Detaillierte Erörterung der Einstellungen 223
17.4.1.1 Der Abschnitt [global] 223
17.4.1.2 Der Abschnitt [printers] 226
17.4.1.3 Beliebige Abschnitte [mein_drucker_name] 227
17.4.1.4 Druckbefehle 228
17.4.1.5 Standard-Systemdruckbefehle unter UNIX 229
17.4.1.6 Eigene Druckbefehle 229
17.5 Die Weiterentwicklung des Druckens seit Samba-2.2 231
17.5.1 Point'n'Print-Client-Treiber auf Samba-Servern 232
17.5.2 Der veraltete Abschnitt [printer$] 232
17.5.3 Erstellen der Freigabe [print$] 233
17.5.4 Parameter im Abschnitt [print$] 233
17.5.5 Das Freigabeverzeichnis [print$] 235
17.6 Treiber in [print$] installieren 236
17.6.1 Treiberinstallation mit dem Assistenten für die Druckerinstallation 236
17.6.2 Druckertreiber installieren mit rpcclient 237
17.6.2.1 Identifizieren von Treiberdateien 237
17.6.2.2 Treiberdateien aus [print$]-Freigaben von Windows-Clients erhalten 239
17.6.2.3 Treiberdateien in [print$] installieren 240

17.6.2.4 Bestätigen der Treiberinstallation mit smbclient 241
17.6.2.5 Ausführen von rpcclient mit adddriver 243
17.6.2.6 Ende von adddriver überprüfen 243
17.6.2.7 Treibererkennung in Samba überprüfen 244
17.6.2.8 Spezifische Flexibilität von Treibernamen 245
17.6.2.9 Ausführen von rpcclient mit setdriver 246
17.7 Installationsvorgang bei Client-Treibern 247
17.7.1 Treiberinstallation auf dem ersten Client 247
17.7.2 Device-Modus auf neuen Druckern setzen 248
17.7.3 Installation weiterer Client-Treiber 250
17.7.4 Erste Client-Verbindung immer als root oder „*printer admin*“ herstellen 250
17.8 Andere Fallstricke 251
17.8.1 Standarddruckeroptionen für Client-Treiber einstellen 251
17.8.2 Unterstützung einer großen Anzahl von Druckern 253
17.8.3 Neue Drucker mit dem Windows NT-APW hinzufügen 255
17.8.4 Fehlermeldung: „*Cannot connect under a different Name*“ 256
17.8.5 Passen Sie beim Zusammenstellen von Treiberdateien auf 257
17.8.6 Samba- und Drucker-Ports 260
17.8.7 Wie Sie übliche Fehlkonfigurationen von Client-Treibern vermeiden 260
17.9 Das Tool-Set Imprints 260
17.9.1 Was ist Imprints? 261
17.9.2 Druckertreiberpakete erstellen 261
17.9.3 Der Imprints-Server 261
17.9.4 Das Installationsprogramm 261
17.10 Netzwerkdrucker ohne Benutzerinteraktion hinzufügen 262
17.11 Der Befehl addprinter 264
17.12 Migration von klassischem Drucken zu Samba 264
17.13 Druckerinformation in Active Directory oder LDAP veröffentlichen 265
17.14 Häufige Fehler 265
17.14.1 Ich gebe mein root-Passwort ein, erhalte aber keinen Zugang 265
17.14.2 Mein Druckauftrag gelangt ins Spooling-Verzeichnis, geht dann aber verloren 265
17.15 Aktualisierung 266

Chapter 18 UNTERSTÜTZUNG DES CUPS-DRUCKSYSTEMSDIE CUPS-FILTER-ARCHITEKTUR 268
18.1 Einleitung 268
18.1.1 Eigenschaften und Vorzüge 268
18.1.2 Überblick 268
18.2 Grundlegende Konfiguration für die CUPS-Unterstützung 269
18.2.1 Das Verlinken von smbd mit libcups.so 269
18.2.2 Einfache smb.conf-Einstellungen für CUPS 270
18.2.3 Komplexere CUPS-Einstellungen in der smb.conf 271
18.3 Erweiterte Konfiguration 272
18.3.1 Zentrales Spooling vs. „*Peer-to-Peer*“-Druck 272
18.3.2 RawPrint Serving — Hersteller-Treiber auf den Windows-Clients 272
18.3.3 Installation von Windows-Client-Treibern 273
18.3.4 Explizites Aktivieren von „*raw*“-Druck für *application/octet-stream* 273

18.3.5 Die Methoden, um Treiber auf den Server zu laden 274
18.4 Erweitertes intelligentes Drucken durch Download von Postscript-Treibern 275
18.4.1 GDI unter Windows – PostScript auf UNIX 276
18.4.2 Windows-Treiber, GDI und EMF 276
18.4.3 UNIX Druckdatei-Konvertierung und GUI-Grundlagen 276
18.4.4 PostScript und Ghostscript 277
18.4.5 Ghostscript — der Software-RIP für nicht-PostScript-fähige Drucker 279
18.4.6 Spezifikation der PostScript Printer Description (PPD) 280
18.4.7 Verwendung von Windows-formatierten Hersteller-PPDs 280
18.4.8 CUPS verwendet auch PPDs für Nicht-PostScript-Drucker 281
18.4.9 MIME-Typen und CUPS-Filter 282
18.4.10 MIME-Typ-Umwandlungsregeln 283
18.4.11 Überblick über das Filtern 284
18.4.11.1 Anforderungen an Filter 284
18.4.12 Vorfilter (Prefilters") 285
18.4.13 pstops 285
18.4.14 pstoraster 286
18.4.15 imagetops und imagetoraster 287
18.4.16 rasterto [druckerspezifisch] 288
18.4.17 CUPS-Backends 288
18.4.18 Die Rolle von cupsomatic/foomatic 290
18.4.19 Das gesamte Bild 291
18.4.20 mime.convs 291
18.4.21 „*Raw*"-Druck 292
18.4.22 application/octet-stream-Druck 292
18.4.23 PostScript Printer Descriptions (PPDs) für Nicht-PS-Drucker 294
18.4.24 *cupsomatic/foomatic-rip* versus *nativer CUPS*-Druck 295
18.4.25 Beispiele für Filterketten 296
18.4.26 Quellen für CUPS-Treiber/PPDs 297
18.4.27 Das Drucken mit Interface Scripts 298
18.5 Netzwerk-Druck (ausschließlich Windows) 299
18.5.1 Von Windows-Clients auf einen NT-Druck-Server drucken 299
18.5.2 Treiberausführung auf dem Client 299
18.5.3 Treiberausführung auf dem Server 300
18.6 Netzwerk-Druck (Windows-Clients — UNIX/Samba-Druck-Server) 300
18.6.1 Von Windows-Clients auf einen CUPS/Samba-Druck-Server drucken 300
18.6.2 Samba empfängt Aufträge und gibt sie an CUPS weiter 301
18.7 Netzwerk-PostScript-RIP 302
18.7.1 PPDs für Nicht-PS-Drucker auf UNIX 302
18.7.2 PPDs für Nicht-PS-Drucker auf Windows 303
18.8 Windows Terminal Server (WTS) als CUPS-Clients 303
18.8.1 Drucker-Treiber, die im „*Kernel-Modus*" laufen, verursachen viele Probleme 303
18.8.2 Workarounds bringen massive Einschränkungen 303
18.8.3 CUPS: Ein „*Stein der Weisen*"? 304
18.8.4 PostScript-Treiber ohne größere Probleme — sogar im Kernel-Modus 304
18.9 Das Konfigurieren von CUPS für den Download von Treibern 304
18.9.1 *cupsaddsmb*: Das unbekannte Hilfsmittel 305

18.9.2 Bereiten Sie Ihre smb.conf für cupsaddsmb vor 305
18.9.3 CUPS „*PostScript-Treiber für Windows NT/200x/XP*“ 305
18.9.4 Das Erkennen verschiedener Treiber-Dateien 307
18.9.5 Das Beschaffen der Adobe-Treiber-Dateien 308
18.9.6 ESP Print Pro PostScript-Treiber für Windows NT/200x/XP 308
18.9.7 Vorbehalte(((Fallstricke ?))), die zu berücksichtigen sind 309
18.9.8 Windows CUPS-PostScript-Treiber versus Adobe-Treiber 310
18.9.9 Das Ausführen von cupsaddsmb (im Quiet Mode) 311
18.9.11 Wiedersehen mit dem Troubleshooting 322
18.10 Die *.tdb-Dateien für das Drucken 323
18.10.1 Triviale Datenbank-Dateien 323
18.10.2 Binär-Format 324
18.10.3 *.tdb-Dateien verlieren 324
18.10.4 Das Verwenden von tdbbackup 324
18.11 CUPS-Druckertreiber von Linuxprinting.org 325
18.11.1 Erklärungen zu foomatic-rip und Foomatic 326
18.11.1.1 690 „*Perfekte*“ Drucker 326
18.11.1.2 Wie das Druck-HOWTO alles begründete 327
18.11.1.3 Foomatics seltsamer Name 327
18.11.1.4 cupsomatic, pdqomatic, lpdomatic und directomatic 327
18.11.1.5 Die *große Vereinheitlichung* ist erreicht 328
18.11.1.6 Externe Treiberentwicklung 329
18.11.1.7 Foren, Downloads, Tutorials und HOWTOs — auch für Mac OS X und kommerzielles UNIX 330
18.11.1.8 PPDs aus der Foomatic-Datenbank 330
18.11.2 foomatic-rip und Foomatic-PPD-Download und -Installation 331
18.12 Seitenabrechnung mit CUPS 333
18.12.1 Quota einrichten 334
18.12.2 Korrektes und inkorrektes Abrechnen 334
18.12.3 Adobe- und CUPS-PostScript-Treiber für Windows-Clients 334
18.12.4 Die Syntax der Datei page_log 335
18.12.5 Mögliche Mängel 335
18.12.6 Zukünftige Entwicklungen 336
18.13 Zusätzliches Material 336
18.14 Auto-Löschen oder Erhaltung der CUPS-Spool-Dateien 338
18.14.1 Erklärung von CUPS-Konfigurationseinstellungen 338
18.14.2 Vorbedingungen 338
18.14.3 Manuelle Konfiguration 339
18.15 Aus CUPS auf Windows-Drucker drucken 339
18.16 Mehr CUPS-Filterketten 341
18.17 Gängige Fehler 341
18.17.1 Ein Windows 9x/ME-Client kann keinen Treiber installieren 341
18.17.2 „*cupsaddsmb*“ fragt immer wieder nach dem root-Passwort 342
18.17.3 „*cupsaddsmb*“-Fehler 342
18.17.4 Der Client kann sich nicht mit dem Samba-Drucker verbinden 342
18.17.5 Neue Probleme: Wiederverbindung mit anderem Konto unter Windows 200x/XP 342
18.17.11 'rpcclient adddriver' 345

18.17.12 'printing = ...' 346
18.17.13 'cups options = ...' 347
18.17.14 'printcap cache time = ...,' 348
18.17.15 'rpcclient setprintername' 349
18.17.16 'cups server = ...' 349
18.17.17 'VampireDriverFunctions' 349

Chapter 19 STAPELBARE VFS-MODULE 354
19.1 Eigenschaften und Vorzüge 354
19.2 Beschreibung 354
19.3 Enthaltene Module 355
19.3.1 audit 355
19.3.2 extd_audit 355
19.3.3 fake_perms 355
19.3.4 recycle 356
19.3.5 netatalk 357
19.4 Anderweitig verfügbare VFS-Module 357
19.4.1 DatabaseFS 357
19.4.2 vscan 358

Chapter 20 WINBIND: BENUTZUNG VON DOMÄNENKONTEN 359
20.1 Eigenschaften und Vorzüge 359
20.2 Einführung 360
20.3 Was Winbind anbietet 361
20.3.1 Zielgruppen 361
20.4 Wie Winbind arbeitet 362
20.4.1 Microsoft Remote Procedure Calls 362
20.4.2 Microsoft Active Directory 362
20.4.3 Name Service Switch 363
20.4.4 Pluggable Authentication Modules 363
20.4.5 Zuordnung von Benutzer- und Gruppen-IDs 364
20.4.6 Das Cachen der Resultate 364
20.5 Installation und Konfiguration 365
20.5.1 Einführung 365
20.5.2 Anforderungen 365
20.5.3 Testen 365
20.5.3.1 Konfigurieren Sie nsswitch.conf und die Winbind-Bibliotheken unter Linux und Solaris 366
20.5.3.2 NSS Winbind auf AIX 367
20.5.3.3 Das Konfigurieren von smb.conf 367
20.5.3.4 Den Samba-Server der Domäne des PDCs anschließen 367
20.5.3.5 Starten und Testen des winbindd-Daemons 367
20.5.3.6 Die init.d-Startskripten anpassen 369
20.5.3.7 Winbind und PAM konfigurieren 372
20.6 Zusammenfassung 376
20.7 Gängige Fehler 376
20.7.1 Warnung vor Problemen durch NSCD 376
20.7.2 Winbind löst keine Benutzer- und Gruppen-Namen auf 377

Chapter 21 FORTGESCHRITTENES NETZWERK-MANAGEMENT 378
21.1 Eigenschaften und Vorzüge 378
21.2 Server-Fernwartung 378
21.3 Desktop-Fernwartung 379
21.3.1 Fernwartung von NoMachine.Com 379
21.4 Die „*Magie*“ von Netzwerk-Anmeldeskripten 380
21.4.1 Hinzufügen von Druckern ohne Benutzer-Eingriff 383

Chapter 22 SYSTEM UND ZUGRIFFSRICHTLINIEN 384
22.1 Eigenschaften und Vorzüge 384
22.2 Anlegen und Verwalten von System-Richtlinien 385
22.2.1 Windows 9x/ME-Richtlinien 385
22.2.2 Windows NT4-Richtlinien-Dateien 386
22.2.2.1 Die Registry „*verderben*“ 386
22.2.3 MS Windows 200x/XP Professional-Richtlinien 387
22.2.3.1 Administration von Windows 200x/XP-Richtlinien 388
22.3 Zugriffs/Benutzer-Richtlinien verwalten 388
22.4 Verwaltungswerkzeuge 389
22.4.1 Der Samba-Werkzeug-Satz Editreg 390
22.4.2 Windows NT4/200x 390
22.4.3 Samba-PDC 390
22.5 Übersicht über den Systemstart und die Anmeldevorgänge 390
22.6 Gängige Fehler 391
22.6.1 Die Richtlinie arbeitet nicht 391

Chapter 23 DAS MANAGEMENT VON DESKTOP-PROFILEN 393
23.1 Eigenschaften und Vorzüge 393
23.2 Roaming Profiles 393
23.2.1 Die Konfiguration von Samba für den Umgang mit Profilen 394
23.2.1.1 NT4/200x-Benutzer-Profile 394
23.2.1.2 Windows 9x/Me-Benutzer-Profile 394
23.2.1.3 Gemischte Windows 9x/Me- und Windows NT4/200x-Benutzer-Profile 395
23.2.1.4 Die Unterstützung von Roaming Profiles deaktivieren 395
23.2.2 Informationen zur Konfiguration von Windows-Client-Profilen 396
23.2.2.1 Windows 9x/Me-Profil-Setup 396
23.2.2.2 Windows NT4 Workstation 398
23.2.2.3 Windows 2000/XP Professional 399
23.2.3 Das gemeinsame Nutzen von Profilen mit Windows 9x/Me- und NT4/200x/XP-Workstations 401
23.2.4 Migration von Profilen von Windows NT4/200x Server zu Samba 401
23.2.4.1 Windows NT4-Werkzeuge zur Profil-Verwaltung 401
23.2.4.2 Randbemerkungen 402
23.2.4.3 moveuser.exe 402
23.2.4.4 Die SID erhalten 402
23.3 Zwingende Profile 402
23.4 Das Anlegen und Verwalten von Gruppen-Profilen 403
23.5 Standard-Profile für Windows-Benutzer 404

23.5.1 MS Windows 9x/Me 404
23.5.1.1 Behandlung von Benutzerprofilen mit Windows 9x/Me 404
23.5.2 MS Windows NT4 Workstation 404
23.5.3 MS Windows 200x/XP 407
23.6 Gängige Fehler 409
23.6.1 Das Konfigurieren von „*Roaming Profiles*“ für einige wenige Benutzer oder Gruppen 409
23.6.2 Ich kann keine Roaming Profiles verwenden 410
23.6.3 Das Standard-Profil verändern 411

Chapter 24 PAM-BASIERTE VERTEILTE AUTHENTIFIZIERUNG 413
24.1 Eigenschaften und Vorzüge 413
24.2 Technische Ausarbeitung 415
24.2.1 PAM-Konfigurationssyntax 415
24.2.1.1 Eigenschaften der Einträge in /etc/pam.d 415
24.2.2 Beispiel einer System-Konfiguration 420
24.2.2.1 PAM: Original-Login-Konfiguration 420
24.2.2.2 PAM: Login mit Verwendung von pam_smbpass 420
24.2.3 Die Konfiguration von PAM in smb.conf 422
24.2.4 Entfernte CIFS-Authentifizierung mitwinbindd.so 422
24.2.5 Passwort-Synchronisation mit pam_smbpass.so 423
24.2.5.1 Konfiguration der Passwort-Synchronisation 423
24.2.5.2 Konfiguration der Passwort-Migration 424
24.2.5.3 Ausgereifte Passwort-Konfiguration 425
24.2.5.4 Konfiguration zur Integration von Kerberos-Passwörtern 425
24.3 Häufige Fehler 426
24.3.1 pam_winbind-Problem 426
24.3.2 Winbind löst Benutzer und Gruppen nicht auf 426

Chapter 25 SAMBA IN MS-WINDOWS-NETZWERKE INTEGRIEREN 428
25.1 Fähigkeiten und Möglichkeiten 428
25.2 Hintergrundinformation 429
25.3 Namensauflösung in einem reinen UNIX/Linux-Umfeld 429
25.3.1 /etc/hosts 429
25.3.2 /etc/resolv.conf 430
25.3.3 /etc/host.conf 431
25.3.4 /etc/nsswitch.conf 431
25.4 Namensauflösung in einem MS Windows-Netzwerk 432
25.4.1 Der NetBIOS-Name-Cache 433
25.4.2 Die Datei LMHOSTS 434
25.4.3 Die Datei HOSTS 436
25.4.4 DNS-Lookup 436
25.4.5 WINS-Lookup 436
25.5 Häufige Fehler 436
25.5.1 Ping funktioniert nur in eine Richtung 437
25.5.2 Sehr langsame Netzwerkverbindungen 437
25.5.3 Ein Problem bei der Namensänderung des Samba-Servers 437

Chapter 26 UNICODE/ZEICHENSÄTZE **439**
26.1 Eigenschaften und Vorzüge 439
26.2 Was sind Charsets und Unicode? 439
26.3 Samba und Zeichensätze 440
26.4 Konvertierung von alten Namen 440
26.5 Japanische Zeichensätze 440
26.5.1 Grundlegende Parameter-Einstellungen 441
26.5.2 Individuelle Implementierungen 444
26.5.3 Migration von Samba-2.2 445
26.6 Gängige Fehler 445
26.6.1 CP850.so kann nicht gefunden werden 445

Chapter 27 BACKUP-TECHNIKEN **446**
27.1 Eigenschaften und Vorzüge 446
27.2 Diskussion von Backup-Lösungen 446
27.2.1 BackupPC 447
27.2.2 Rsync 447
27.2.3 AMANDA 448
27.2.4 BOBS: Browseable Online Backup System 448

Chapter 28 HOCHVERFÜGBARKEIT **449**
28.1 Eigenschaften und Vorzüge 449
28.2 Technische Beschreibung 449
28.2.1 Das ultimative Ziel 450
28.2.2 Warum ist dies so schwer? 450
28.2.2.1 Die Frontend-Herausforderung 451
28.2.2.2 De-Multiplexen von SMB-Anfragen 451
28.2.2.3 Die Herausforderung 'Verteiltes Dateisystem' 451
28.2.2.4 Restriktive Zwänge in verteilten Dateisystemen 452
28.2.2.5 Serverpool-Kommunikation 452
28.2.2.6 Anforderungen an die Serverpool-Kommunikation 452
28.2.2.7 Benötigte Änderungen an Samba 452
28.2.3 Eine einfache Lösung 453
28.2.4 Hochverfügbarkeits-Serverprodukte 453
28.2.5 MS-DFS: Der Arme-Leute-Cluster 454
28.2.6 Schlussfolgerungen 454

Part IV Migration und Updating **453**

Chapter 29 UPGRADE VON SAMBA-2.X AUF SAMBA-3.0.0 **455**
29.1 Kurzanleitung zur Migration 455
29.2 Neue Features in Samba-3 455
29.3 Änderungen von Konfigurationsparametern 456
29.3.1 Enfernte Parameter 456
29.3.2 Neue Parameter 457
29.3.3 Geänderte Parameter (Änderungen im Verhalten): 459
29.4 Neue Funktionalität 460

29.4.1 Datenbanken 460
29.4.2 Änderungen im Verhalten 460
29.4.3 Passdb-Backends und Authentifikation 461
29.4.4 LDAP 461
29.4.4.1 Neues Schema 461
29.4.4.2 Neues Suffix für die Suche 462
29.4.4.3 Idmap-LDAP-Support 463

Chapter 30 MIGRATION VON EINEM NT4-PDC AUF EINEN SAMBA-3-PDC 464
30.1 Planung und Beginn 464
30.1.1 Zielsetzungen 464
30.1.1.1 Domänen-Entwurf 466
30.1.1.2 Entwurf der Server-Freigaben und -Verzeichnisse 466
30.1.1.3 Anmelde-Skripten 467
30.1.1.4 Anlegen und Migration von Profilen 467
30.1.1.5 Benutzer- und Gruppen-Konten 467
30.1.2 Schritte im Migrationprozess 468
30.2 Migrationsoptionen 468
30.2.1 Den Erfolg planen 469
30.2.2 Wahlmöglichkeiten bei der Samba-3-Implementation 469

Chapter 31 SWAT — DAS SAMBA-ADMINISTRATIONS-WERKZEUG 472
31.1 Eigenschaften und Vorzüge 472
31.2 Grundlagen und technische Hilfen 473
31.2.1 Überprüfen der SWAT-Installation 473
31.2.1.1 Lokalisieren der Datei swat 473
31.2.1.2 Lokalisieren der Hilfedateien zu SWAT 474
31.2.2 SWAT aktivieren 475
31.2.3 Absichern von SWAT mit SSL 476
31.2.4 Die Mehrsprachenunterstützung von SWAT aktivieren 477
31.3 Übersicht und ein Schnelldurchlauf 478
31.3.1 Die Homepage von SWAT 478
31.3.2 Globale Einstellungen 478
31.3.3 Einstellungen zur Freigabe (Share) 479
31.3.4 Druckereinstellungen 479
31.3.5 Der SWAT-Wizard 479
31.3.6 Die Status-Seite 480
31.3.7 Die Übersichtsseite 480
31.3.8 Die Seite zur Passwortänderung 480
31.4 Fehlerhafte Ausgaben der Übersichtsseite von SWAT 480

Part V Troubleshooting 479

Chapter 32 DIE SAMBA-CHECKLISTE 481
32.1 Einleitung 481
32.2 Vorbemerkung 481

32.3 Die Tests 482

Chapter 33 ANALYSE UND LÖSUNG VON PROBLEMEN MIT SAMBA 488
33.1 Diagnose-Tools 488
33.1.1 Das Debuggen mit Samba selbst 488
33.1.2 Tcpdump 489
33.1.3 Ethereal 489
33.1.4 Der Windows Netzwerk-Monitor 490
33.1.4.1 Installieren des Netzwerk-Monitors auf einer NT-Workstation 490
33.1.4.2 Installieren des Netzwerk-Monitors unter Windows 9x/Me 491
33.2 Hilfreiche URLs 491
33.3 Hilfe aus Mailing-Listen erhalten 491
33.4 Wie man aus Mailinglisten rauskommt 492

Chapter 34 DAS MELDEN VON FEHLERN 493
34.1 Einführung 493
34.2 Allgemeine Informationen 493
34.3 Debug-Level 494
34.4 Interne Fehler 494
34.5 Sich an einen laufenden Prozess anschließen 495
34.6 Patches 495

Part VI Anhang 495

Chapter 35 WIE MAN SAMBA KOMPILIERT 497
35.1 Der Zugriff auf den Source-Code von Samba über Subversion 497
35.1.1 Einführung 497
35.1.2 Der Subversion-Zugriff auf samba.org 497
35.1.2.1 Zugriff via SVNweb 497
35.1.2.2 Zugriff via Subversion 498
35.2 Zugriff auf die Samba-Quelltexte mit rsync und ftp 498
35.3 Überprüfen der PGP-Signatur von Samba 498
35.4 Kompilieren der Binärdateien 499
35.4.1 Das Kompilieren von Samba mit Active Directory Support 500
35.4.1.1 Die Installation der für Debian erforderlichen Packages 500
35.4.1.2 Die Installation der für Red Hat Linux erforderlichen Packages 501
35.4.1.3 Package-Anforderungen in SuSE Linux 501
35.5 Starten von smbd und nmbd 501
35.5.1 Starten aus der inetd.conf 501
35.5.2 Alternative: smbd als Daemon starten 503

Chapter 36 PORTABILITÄT 504
36.1 HPUX 504
36.2 SCO UNIX 504
36.3 DNIX 505
36.4 Red Hat Linux 506
36.5 AIX 506
36.5.1 Sequenzieller Read Ahead 506

36.6 Solaris 507
36.6.1 Verbesserungen beim Locking 507
36.6.2 Winbind auf Solaris 9 507

Chapter 37 SAMBA UND ANDERE CIFS-CLIENTS 508
37.1 Macintosh-Clients 508
37.2 OS/2-Clients 508
37.2.1 Das Konfigurieren von OS/2 Warp Connect oder OS/2 Warp 4 508
37.2.2 Andere Versionen von OS/2 konfigurieren 509
37.2.3 Druckertreiber-Download für OS/2-Clients 509
37.3 Windows for Workgroups 510
37.3.1 Neuester TCP/IP-Stack von Microsoft 510
37.3.2 Das Löschen von .pwl-Dateien nach Passwort-Änderungen 510
37.3.3 Den Umgang mit Passwörtern in Windows for Workgroups konfigurieren 510
37.3.4 Groß-/Kleinschreibung in Passwörtern 511
37.3.5 TCP/IP als Standard-Protokoll verwenden 511
37.3.6 Geschwindigkeitssteigerung 511
37.4 Windows 95/98 511
37.4.1 Geschwindigkeitssteigerung 512
37.5 Windows 2000 Service Pack 2 512
37.6 Windows NT 3.1 513

Chapter 38 PERFORMANCE-TUNING FÜR SAMBA 514
38.1 Vergleiche 514
38.2 Socket-Optionen 514
38.3 Read Size 515
38.4 Max Xmit 515
38.5 Log-Level 516
38.6 Read Raw 516
38.7 Write Raw 516
38.8 Slow Logins 516
38.9 Client-Tuning 516
38.10 Samba-Performance-Problem nach dem Wechsel des Linux-Kernels 516
38.11 Beschäigte tdb-Dateien 517
38.12 Samba-Performance ist sehr langsam 517

Chapter 39 DNS UND DHCP: KONFIGURATIONSANLEITUNG 519
39.1 Eigenschaften und Vorzüge 519
39.2 Beispielkonfiguration 520
39.2.1 Dynamisches DNS 520
39.2.2 DHCP-Server 524

Chapter 40 WEITERE HILFSQUELLEN 525
40.1 Webseiten 525
40.2 Verwandte Updates von Microsoft 526

SUBJECT INDEX 527

Stichwortverzeichnis 527

Teil I

Grundlegende Installation

VORBEREITUNG ZUR SAMBA-KONFIGURATION

Dieser Abschnitt der Samba-HOWTO-Sammlung beinhaltet grundlegende Informationen darüber, wie man die Teile von Samba installiert und konfiguriert, die Sie am meisten nutzen. BITTE lesen Sie dies.

Kapitel 1

EINFÜHRUNG IN SAMBA

„*Wenn du verstehst, was du tust, wirst du nichts lernen – Anonym*“

Samba ist ein Datei- und Druckserver Windows-basierende Clients, die TCP/IP als Transport-Protokoll nutzen. Tatsächlich kann es jeden SMB/CIFS-aktiven Client unterstützen. Eine von Sambas großen Stärken ist, dass Sie in der Lage sind, Ihre Windows- und Linux-Maschinen zusammen zu nutzen, ohne einen separaten Windows NT/2000/2003-Server zu benötigen. Samba wird derzeit von einem 30-köpfigen Team von Programmierern entwickelt. Es wurde ursprünglich von Andrew Tridgell entwickelt.

1.1 Hintergrund

Vor langer Zeit gab es ein Schlüsselwort welches sich auf DCE/RPC bezog. Es stand für „*Computing Environment/Remote Procedure Calls*“ und war vom Konzept her eine gute Idee. Ursprünglich wurde es von Apollo/HP als NCA1.0 (Network Computing Architecture) entwickelt und konnte nur über UDP benutzt werden. Als es nötig wurde, das Ganze über TCP zu betreiben, um die Kompatibilität zu DECnet3.0 gewährleisten zu können, wurde es neu entworfen, zur Organisation „*The Open Group*“ gesandt und offiziell als DCE/RPC bekannt. Microsoft kam allerdings auf die Idee, mehr als $20 für eine Arbeitsplatz-Lizenz zu verlangen und es als eigenes MSRPC zu verkaufen. Von diesem Punkt an wurde das Konzept in Form von SMB (Server Message Block, das „*Was*“) unter Benutzung von NetBIOS (Network Basic Input/Output System, das „*Wie*“) als Kompatibilitätsschicht weiter geführt. Sie können SMB über viele verschiedene Protokolle nutzen, sprich transportieren; viele verschiedene Implementationen führen zu einem Ergebnis, einschließlich NBIPX (NetBIOS über IPX, NwLnkNb oder NWNBLink) und NBT (NetBIOS über TCP/IP oder NetBT). Über die Jahre hinweg wurde NBT zur meistgenutzten Form der Implementationen bis zum Fortschritt des „*Direct-Hosted TCP*“ – der Microsoft-Marketing-Formulierung zur vollständigen Eliminierung von NetBIOS und der Möglichkeit, SMB direkt an den TCP-Port 445 zu binden. Wie es zum jetzigen Zeitpunkt aussieht, muss „*Direct-Hosted TCP*“ jedoch noch aufschließen.

Die wohl beste Abhandlung über den Ursprung von SMB erschien 1997 in einem Artikel mit dem Titel - „*CIFS: Common Insecurities Fail Scrutiny*“.

Mehrere Megabytes aus NT-Security-Archiven, verschiedensten Whitepapers, RFCs, der CIFS-Spezifikation, dem Samba-Zeug, ein paar MS-Knowledge-Base-Artikel, Zeichenketten

*aus Binärdateien und Packet-Dumps wurden pflichtbewußt in den Phasen der Informationssammlung dieses Projektes durchgeackert, und es fehlen noch *immer* einige Teile ... Oftmals beschwerlich, wurde der Weg zumindest großzügig gesäumt von Anlässen zum* „Hand vor die Stirn schlagen*“ und dem Murmeln von* „Mein Gott, was denken die sich dabei?*“.*

1.2 Fachsprache

- SMB: Akronym für „*Server Message Block*“. Dies ist das Datei- und Druckerfreigabe-Protokoll von Microsoft.
- CIFS: Akronym für „*Common Internet File System*“. Um 1996 entschied Microsoft, dass SMB das Wort „*Internet*“ im Namen bräuchte, und änderte den Namen in CIFS.
- Direct-Hosted: Eine Methode, Datei/Drucker-Freigabedienste über Port 445/tcp zur Verfügung zu stellen. Hierbei wurde nur DNS statt WINS zur Auflösung der Namen in IP-Adressen benutzt.
- IPC: Akronym für „*Inter-Process Communication*“. Eine Methode, spezielle Informationen unter Programmen zu verbreiten.
- Marshalling: Eine Methode zur sequenziellen Sortierung von variablen Daten, passend zur Übertragung über eine Netzwerkverbindung bzw. Speicherung in eine Datei. Die Quelldateien können durch einen ähnlichen Prozess namens Unmarshalling wiederhergestellt werden.
- NetBIOS: Akronym für „*Network Basic Input/Output System*“. Dies ist kein Protokoll; es ist eine Möglichkeit der Kommunikation über ein anderes Protokoll. Dies ist ein Standard, der ursprünglich 1983 von IBM entwickelt wurde. Um die Analogie ein wenig zu übertreiben, könnte man NetBIOS mit dem BIOS Ihres Rechners vergleichen. Ihr BIOS kontrolliert die Ein-/Ausgabe der Hardware Ihres Rechners, und NetBIOS kontrolliert die Ein-/Ausgaben über das Netzwerk. Nochmals: Dies ist eine kleine Übertreibung, sollte aber helfen, dieses Paradigma verständlich zu machen. Was wichtig ist, ist die Tatsache, dass NetBIOS kein Protokoll, sondern ein Übermittlungsstandard ist. Leider tendieren auch technisch versierte Leute dazu, ohne viel darüber nachzudenken, NetBIOS mit NetBEUI zu verwechseln.
- NetBEUI: Akronym für das „*NetBIOS Extended User Interface*“. NetBEUI ist nicht mit NetBIOS vergleichbar. Es ist ein Protokoll, kein Standard. Es ist auch kein routingfähiges Protokoll, was wiederum heißt, dass es nicht von einer Seite eines Routers auf die andere gelangt. Es ist nicht notwendig, NetBEUI zu verstehen, um SMB zu entziffern; es hilft zu verstehen, dass NetBEUI nicht das Gleiche wie NetBIOS ist, um Ihre Beliebtheit auf Parties zu erhöhen. Auf NetBEUI wurde ursprünglich von Microsoft als „*NBF*“ oder „*Der Windows NT NetBEUI Frame Protocol Treiber*“ verwiesen. Heutzutage hört man nicht mehr viel davon.
- NBT: Akronym für „*NetBIOS über TCP*“ auch bekannt als „*NetBT*“. Erlaubt die Benutzung von NetBIOS-Verkehr im TCP/IP. Im Endeffekt werden NetBIOS-Namen zu IP-Adressen umgewandelt und NetBIOS-Namenstypen sind im Grunde genommen mit TCP/IP-Ports vergleichbar. So werden in Windows 95/98/ME die Datei- und Druckerfreigaben verwirklicht. Traditionell sind sie an drei Ports gebunden: NetBIOS

Name Service (nbname) über UDP Port 137, NetBIOS Datagram Service (nbdatagram) über UDP Port 138 und der NetBIOS Session Service (nbsession) über TCP Port 139. Jegliche Namensauflösung wird über WINS erledigt, NetBIOS-Broadcasts (Anm. des Übersetzers: Broadcasts sind Netzwerkaufrufe an alle anderen Stationen im Umkreis) und DNS. NetBIOS über TCP wird im RFC 1001 (Konzepte und Methoden) und RFC 1002 (Detaillierte Spezifikationen) beschrieben.

- W2K: Akronym für Windows 2000 Professional oder Server
- W3K: Akronym für Windows 2003 Server

Wenn Sie Hilfe benötigen, wenden Sie sich bitte an die Samba-Mailing-Liste (erreichbar über http://www.samba.org <`http://www.samba.org/`>).

1.3 Verwandte Projekte

Derzeit gibt es zwei weitere Netzwerk-Dateisystem-Client-Projekte für Linux, die direkt mit Samba in Verbindung stehen: SMBFS und CIFS VFS. Sie sind beide im Linux-Kernel verfügbar.

- SMBFS (Server Message Block File System) erlaubt es, SMB-Freigaben unter Linux zu mounten (binden); das Protokoll, das Microsoft Windows und OS/2 Lan Manager zur Freigabe von Dateien und Druckern über lokale Netzwerke verwenden, lässt sich hier nutzen, um entfernte Shares ähnlich wie andere Unix-Verzeichnisse zu binden. Dies ist nützlich, wenn Sie nur solche Dateisysteme mounten wollen, ohne gleich selbst einen SMBFS-Server zu betreiben.
- CIFS VFS (Common Internet File System Virtual File System) ist der Nachfolger von SMBFS und wird derzeit aktiv für die neue Version des Linux-Kernels entwickelt. Dieses Modul soll erweiterte Netzwerkdateisysteme, Funktionen wie Unterstützung von dfs (hierarchischer Namensraum / hierarchical name space), sichere „*Pro-User*“-Sessions, sicheres verteiltes Zwischenspeichern (oplock), optionales Signieren von Paketen, den Unicode-Zeichensatz, weitere internationalisierte Verbesserungen und die optionale Einbindung von Winbind (nsswitch) unterstützen.

Hinweis: Es ist wichtig zu erkennen, dass dies nur Implementationen für Client-Dateisysteme sind, die nichts damit zu tun haben, einen Datei- und Druckserver zu betreiben.

Es gibt noch weitere OpenSource-CIFS-Client-Tools, wie zum Beispiel das jCIFS Projekt <`http://jcifs.samba.org/`> welches ein in Java geschriebenes SMB-Client-Toolkit zur Verfügung stellt.

1.4 SMB-Methodologie

Traditionell nutzt SMB den UDP-Port 137 (NetBIOS name service oder netbios-ns), den UDP-Port 138 (NetBIOS datagram service oder netbios-dgm) und den TCP-Port 139 (NetBIOS session service oder netbios-ssn). Jeder, der mit einem guten Netzwerk-Packet-Analyzer sein Netzwerk beobachtet, wird über die Menge an Verkehr amüsiert sein, der ausgelöst wird, wenn man nur eine einzige Datei öffnet. Grundsätzlich werden SMB-Sitzungen/Sessions in folgender Reihenfolge aufgebaut:

- „*TCP-Verbindung*“ - Aufbau des 3-Wege-Handschlags (Verbindung) zu Port 139/tcp oder 445/tcp.
- „*NetBIOS-Session-Anfrage*“ - Benutzt folgende Rufnamen: Den lokalen NetBIOS-Namen der lokalen Maschine zzgl. des 16. Buchstabens 0x00 und den NetBIOS-Namen des Servers zzgl. 0x20 als 16. Buchstaben.
- „*SMB Negotiate Protocol*“ - bestimmt den Protokoll-Dialekt, der benutzt werden soll. Dieser Dialekt kann einer der folgenden sein: PC Network Program 1.0 (Core) - nur share level security modus; Microsoft Networks 1.03 (Core Plus) - nur share level security modus; Lanman1.0 (LAN Manager 1.0) - nutzt Challenge/Response Authentication; Lanman2.1 (LAN Manager 2.1) - nutzt Challenge/Response Authentication; NT LM 0.12 (NT LM 0.12) - nutzt Challenge/Response Authentication.
- SMB Session Startup. Passwörter werden nach folgenden Methoden verschlüsselt (oder auch nicht): Null (keine Verschlüsselung); Cleartext/Klartext (keine Verschlüsselung); LM und NTLM; NTLM; NTLMv2.
- SMB Tree Connect: Verbindung zu einem Freigabenamen (z.B., \\servername\share); Verbindung zu einem Servicenamen (z.B., IPC$).

Eine gute Art, diesen Prozess zu untersuchen, besteht darin, das SWB Program von SecurityFriday <`http://www.securityfriday.com/ToolDownload/SWB/swb_doc.html`> auszuprobieren. Es ermöglicht Ihnen, Schritt für Schritt durch eine SMB/CIFS-Sitzung zu gehen.

1.5 Epilog

„*Was grundlegend falsch ist, ist, dass niemand daran Geschmack finden kann, wenn er es nicht probiert hat. Microsoft hat stark daran gearbeitet, die Oberfläche schön zu gestalten, nur intern ist es eine komplette Unordnung. Auch Mitarbeiter von Microsoft, die seit Jahren dort arbeiten und viel Erfahrung mit sich bringen, haben keine Ahnung, was intern wirklich abläuft. Schlimm, dass niemand sich traut, dies zu ändern. Niemand traut sich, einen Bug zu fixen, nur weil die Gefahr besteht, dass dieser Fix Hunderte von Programmen zum Absturz bringen könnte. Dazu kommt, dass Microsoft nicht daran interessiert ist, Bugs zu fixen – sie sind vielmehr daran interessiert, Geld zu machen. Sie haben niemanden, der stolz ist, in Windows 95 ein Betriebssystem zu sehen.*“

„*Die Leute von Microsoft wissen, dass es ein schlechtes Betriebssystem ist, und arbeiten weiter daran, weil sie die nächste Version auf den Markt bringen wollen, um all die neuen Möglichkeiten des Systems verkaufen zu können.*“

„*Das Problem hierbei ist, dass Sie über die Zeit Verständnis hierfür entwickeln, ohne es zu verstehen, da niemand WIRKLICH Probleme behebt, ist das Endergebnis stark verpfuscht. Sie können dem System nicht vertrauen, da es unter bestimmten Bedingungen einfach spontan neu startet oder einfach nur stehen bleibt, wenn Sie gerade etwas völlig Normales machen. Normalerweise funktioniert es gut, nur ist es irgendwann ohne Begründung tot, und niemand weiß warum. Nicht Microsoft, nicht die erfahrenen Anwender und schon gar nicht der ahnungslose Benutzer, der vor seinem Bildschirm sitzt und sich fragt:* ‚Was hab ich bloß falsch gemacht?‘*, wenn er doch gar nichts falsch gemacht hat.*“

„*Das ist es, was mich wirklich irritiert.*“

– Linus Torvalds, in einem Interview mit dem BOOT Magazin, September 1998 <http://hr.uoregon.edu/davidrl/boot.txt>

Kapitel 2

WIE MAN SAMBA INSTALLIERT UND TESTET

2.1 Wie man Samba bekommt und installiert

Binäre Pakete von Samba gibt es mittlerweile in fast jeder Linux- oder Unix-Distribution. Es gibt auch einige Pakete auf der Samba-Homepage <`http://samba.org/`>. Lesen Sie bitte in der Bedienungsanleitung Ihres Betriebssystems nach, wie Sie auf Ihrem System Samba installieren können.

Wenn Sie Samba von den Quelldateien selbst installieren möchten, bekommen Sie hier weitere Informationen.

2.2 Samba konfigurieren (smb.conf)

Die Samba-Konfiguration wird in der Datei `smb.conf` vorgenommen, die Sie üblicherweise unter `/etc/samba/smb.conf` oder `/usr/local/samba/lib/smb.conf` finden. Sie können diese Datei selbst editieren oder eine der vielen grafischen Oberflächen nutzen, wie das webbasierte SWAT, das mit Samba mitgeliefert wird.

2.2.1 Die Syntax der Konfiguration

Die `smb.conf` nutzt nahezu die gleiche Syntax wie die verschiedenen ini-Dateien von Windows 3.1: Jede Datei enthält verschiedene Abschnitte, wobei diese Abschnitte durch Klammern ([]) getrennt sind. Jeder Abschnitt besteht aus keinem oder mehreren Schlüssel/Wert-Paaren, die durch das Gleichheitszeichen (=) miteinander verbunden werden. Dies ist eine Klartext-ASCII-Datei, die Sie mit ihrem Lieblingseditor bearbeiten können.

Jeder Abschnitt der Datei `smb.conf` repräsentiert eine Freigabe auf dem Samba-Server, bis auf den Abschnitt „*global*“. Dieser ist ein spezieller Abschnitt, da er Einstellungen enthält, die den gesamten Samba-Server beeinflussen und nicht nur einzelne Freigaben.

Beispiel 2.2.1 enthält eine sehr kleine `smb.conf`.

Beispiel 2.2.1. Eine minimale smb.conf

```
[global]
        workgroup = WKG
        netbios name = MYNAME

[share1]
        path = /tmp

[share2]
        path = /my_shared_folder
        comment = Some random files
```

2.2.2 Samba starten

Samba an sich besteht aus zwei oder drei so genannten Daemons. Ein Daemon ist eine Unix-Applikation, die im Hintergrund läuft und Dienste zur Verfügung stellt. Ein Beispiel für einen solchen Dienst ist der Apache Webserver, für den der Daemon **httpd** heißt. Im Falle von Samba gibt es drei Daemons, von denen mindestens zwei benötigt werden.

Der Samba-Server besteht aus folgenden Daemons:

nmbd Dieser Daemon behandelt alle Namensregistrierungen und Anfragen zur Namensauflösung. Es ist das primäre Werkzeug zum Durchsuchen eines Netzwerks. Er ist in der Lage, mit jedem UDP-basierten Protokoll umzugehen. Das Kommando **nmbd** sollte der erste Daemon sein, der im Rahmen des Startvorgangs von Samba geladen wird.

smbd Dieser Daemon behandelt alle TCP/IP-basierenden Verbindungen für datei- und druckbasierende Operationen. **smbd** befasst sich auch mit der Benutzerauthentifikation und sollte direkt nach dem Start von **nmbd** aufgerufen werden.

winbindd Dieser Daemon sollte gestartet werden, wenn der Samba-Server Mitglied einer Windows-NT4- oder ADS-Domäne (ADS = Active Directory Service) ist. Er ist ebenfalls nötig, wenn Samba in einem Vertrauensverhältnis zu anderen Domänen steht.

Wenn Samba als Paket einer Distribution installiert wird, liegt meist ein Start-Stopp-Skript für den ordnungsgemäßen Start von Samba vor. Dies ist aber eher ein positives Merkmal einer Distribution. Bitte konsultieren Sie das Administrationshandbuch Ihres Betriebssystems bezüglich der Einbindung eines solchen Start-Stopp-Skripts.

2.2.3 Beispielkonfiguration

In einem separaten Unterverzeichnis der Distribution gibt es Beispiele von Konfigurationsdateien. Es ist empfehlenswert, diese Beispiele aufmerksam zu lesen, um zu verstehen, wie die

verschiedenen Optionen in der Praxis zusammenarbeiten. Um eine Zusammenfassung aller möglichen Optionen zu sehen, rufen Sie bitte die Manpages auf. Es lohnt sich, die vorgegebene Datei `smb.conf.default` als Grundlage der persönlichen Konfiguration zu verwenden, da sie viele Kommentare zu den verschiedenen Optionen enthält.

Die einfachste Konfiguration sollte mindestens Beispiel 2.2.2 enthalten.

Beispiel 2.2.2. Eine weitere vereinfachte smb.conf-Datei

```
[global]
        workgroup = MITTELERDE

[homes]
        guest ok = no
        read only = no
```

Diese Konfiguration erlaubt es jedem, der einen Benutzeraccount auf dem Server hat, sich unter Verwendung seines Login-Namens mit der Freigabe *homes* zu verbinden. (Hinweis: Der Name der Arbeitsgruppe/Domäne sollte hier so wie gewünscht gesetzt werden; der Standard für diese Option ist WORKGROUP.)

Stellen Sie sicher, dass Sie die Datei `smb.conf` im richtigen Verzeichnis gespeichert haben.

Für weitere Informationen zu den Sicherheitseinstellungen für *[homes]* lesen Sie bitte Kapitel **??** „Samba absichern“.

2.2.3.1 Test der Konfiguration mit testparm

Es ist wichtig, Ihre Konfigurationsänderung mit testparm zu überprüfen. Wenn Ihre Konfiguration richtig ist, sollte testparm eine Liste der verfügbaren Services auflisten, andernfalls wird es eine Fehlermeldung ausgeben. Überprüfen Sie Ihre Konfiguration mit:

```
root#  testparm /etc/samba/smb.conf
```

testparm wird Ihre Konfiguration überprüfen und mögliche unbekannte Parameter oder Fehler in der Syntax ausgeben.

Es ist sehr empfehlenswert, testparm nach einer Änderung der `smb.conf` auszuführen.

2.2.4 SWAT

SWAT ist eine Weboberfläche, mit der die Konfiguration von Samba einfacher wird. Es kann möglich sein, dass SWAT nicht in der Paketinstallation Ihrer Distribution enthalten ist. Dann finden Sie es aber meist in einem separaten Paket. Bitte beachten Sie die SWAT-Manpage, wenn Sie SWAT aus den Quelldateien kompilieren, installieren und konfigurieren wollen.

Um SWAT zu starten, verwenden Sie einfach Ihren liebsten Webbrowser und folgende URL <http://localhost:901/>. Ersetzen Sie *localhost* durch den Namen des Computers, auf dem Sie Samba installiert haben, wenn Sie den Webbrowser von einem anderen PC als den Samba-Server starten.

SWAT kann von jedem Browser eines IP-Netzes aus genutzt werden, aber beachten Sie, dass bei Verbindungen von einem entfernten Rechner die Gefahr besteht, dass Ihre Passwörter abgehört werden, da diese im Klartext über das Kabel transportiert werden.

Weitere Informationen über SWAT können Sie hier finden: Kapitel **??** „SWAT Das Samba-Administrations-Werkzeug“ .

2.3 Auflistung von Freigaben auf dem Server

Verwenden Sie folgenden Befehl, um die verfügbaren Freigaben Ihres Samba-Servers aufzulisten:

```
$ smbclient -L yourhostname
```

Sie sollten nun eine Liste der verfügbaren Freigaben Ihres Servers sehen - wenn nicht, dann ist etwas nicht richtig konfiguriert. Diesen Befehl können Sie ebenfalls nutzen, um die Freigaben anderer Server z.B. Windows 2000 zu betrachten.

Wenn Sie User-level-Sicherheit als Sicherheit für Ihren Server gewählt haben, sollten Sie nach der Eingabe des Befehls nach einem Passwort für Ihren Benutzer gefragt werden, bevor Sie die Auflistung sehen. Lesen Sie die Manpage zu **smbclient** für weitere Informationen dazu. Sie können den Befehl mit der Option `-N` dazu bringen, auch ohne Passwort die Freigabeliste anzuzeigen.

2.4 Verbindung zu einem UNIX-Client aufbauen

Verwenden Sie folgenden Befehl:

```
$ smbclient  //ihrhostname/eindienst
```

Normalerweise ist *ihrhostname* der Name des Hosts, auf dem sich der smbd befindet, und *eindienst* ist ein beliebiger Dienst, den dieser Host zur Verfügung stellt. Versuchen Sie es mit Ihrem Benutzernamen, wenn Sie einen Abschnitt *[homes]* in Ihrer `smb.conf` haben.

Beispiel: Wenn der UNIX-Host *bambi* heißt und ein gültiger Login-Name *fred* ist, könnten Sie Folgendes schreiben:

```
$ smbclient //bambi/fred
```

2.5 Verbindung von einem entfernten SMB-Client

Nun, da Samba lokal richtig funktioniert, können Sie versuchen, sich von einem anderen Rechner aus an Ihrem Samba-Server anzumelden. Innerhalb weniger Minuten sollte der Samba-Server in der Netzwerkumgebung Ihres Windows-Subnetzes sichtbar sein. Versuchen Sie, Ihren Samba-Server dort zu finden, oder versuchen Sie, eine Netzwerkverbindung mit Ihrem Server herzustellen.

Um eine Netzwerkverbindung unter DOS, Windows oder OS/2 herzustellen, führen Sie folgenden Befehl aus:

```
C:\> net use d: \\servername\dienst
```

Versuchen Sie zu drucken:

```
C:\> net use lpt1:   \\servername\druckdienst

C:\> print filename
```

2.6 Was tun, wenn etwas nicht funktioniert?

Sie können hier Hilfe finden oder aber, wenn es danach immer noch nicht funktioniert, lesen Sie bitte Kapitel **??** „Analyse und Lösung von Problemen mit Samba“. Samba wurde bereits auf Tausenden von Systemen installiert, daher könnte es hilfreich sein, im Internet zu recherchieren, ob jemand anderes auch ihr Problem hatte und einen Weg gefunden hat, es zu lösen.

2.7 Häufige Fehler

Folgende Fragen und Themen tauchen immer wieder in der Samba-Mailing-Liste auf.

2.7.1 Große Anzahl von smbd-Prozessen

Samba enthält drei Kern-Programme: nmbd ist der Namensserver-Daemon, smbd ist der Server-Message-Daemon, und winbindd ist der Daemon, der mit Domänen-Controllern arbeitet.

Wenn Samba *nicht* als WINS-Server fungiert, sollte es nur eine Instanz des nmbd-Daemons auf Ihrem System geben. Andernfalls sollten zwei nmbd-Prozesse laufen, von denen einer die WINS-Anfragen behandelt.

smbd behandelt alle Verbindungsanfragen. Er ruft sich selbst für jede neue Client-Verbindung auf. Das ist der Grund, warum Sie mehrere Prozesse von smbd sehen können, nämlich einen für jede Client-Verbindung.

winbindd läuft in einem oder zwei Prozessen, abhängig davon, ob er im *split mode* läuft (in diesem Fall hat er zwei Instanzen).

2.7.2 Fehlermeldung: open_oplock_ipc

Eine Fehlermeldung wird in der Log-Datei beim Starten von smbd angezeigt: „*open_oplock_ipc: Failed to get local UDP socket for address 100007f. Error was Cannot assign requested.*“

Ihr Loopback-Interface funktioniert nicht korrekt. Vergewissern Sie sich, dass es korrekt konfiguriert wurde. Das Loopback-Interface ist eine interne (virtuelle) Netzwerkkarte mit der IP-Adresse *127.0.0.1*. Lesen Sie in der Dokumentation Ihres Betriebssystems nach, wie Ihr Loopback-Interface einzurichten ist.

2.7.3 Fehlermeldung:„*The network name cannot be found*“

Dieser Fehler kann von folgenden Fehlkonfigurationen verursacht werden:

- Sie haben einen nicht existenten Pfad für eine Freigabe in der `smb.conf` angegeben.
- Der Benutzer, mit dem Sie versuchen, auf eine Freigabe zuzugreifen, hat nicht die erforderlichen Rechte, um auf den UNIX-Pfad zuzugreifen. Sowohl das Leserecht (r) als auch das Zugriffsrecht (x) sollten dem Benutzer eingeräumt werden.
- Die Freigabe, auf die Sie zuzugreifen versuchen, existiert nicht.

Kapitel 3

SCHNELLSTART: ALLHEILMITTEL FÜR UNGEDULDIGE

Als wir zum ersten Mal nach Vorschlägen für die Aufnahme in die Samba HOWTO-Dokumentation fragten, fragte gleich jemand nach Beispielkonfigurationen — , und zwar nach vielen. Diese Bitte ist jedoch schwierig zu erfüllen, zumal man unserer Einschätzung nach mehr lernt, wenn man sich viele Ausschnitte aus Produktionssystemen anschaut. Dies ist es, was der Rest dieses Dokuments macht: Es zeigt ausführliche Beschreibungen der Konfigurationsmöglichkeiten innerhalb des Kontextes des betroffenen Kapitels. Wir hoffen, dass dieses Kapitel die verlangte „*Medizin*“ ist.

3.1 Eigenschaften und Vorzüge

Samba braucht sehr wenig Konfiguration, um ein arbeitsfähiges Basissystem zu erzeugen. In diesem Kapitel gehen wir vom Einfachen zum Komplexen vor, und für jeden stellen wir alle Schritte und Konfigurationsdateien vor, die benötigt werden, um Samba zum Laufen zu bringen. Bitte beachten Sie, dass ein umfassend konfiguriertes System wahrscheinlich zusätzliche praktische Möglichkeiten ergibt. Die zusätzlichen Möglichkeiten werden im Rest dieses Dokuments behandelt.

Die Beispiele, die hier benutzt werden, haben wir von Leuten erhalten, die Anfragen zu Beispielkonfigurationen gestellt hatten. Alle Identitäten wurden zu deren Schutz verschleiert, und die Ähnlichkeit zu unrealistischen und nicht existierenden Seiten ist beabsichtigt.

3.2 Beschreibung von Beispielseiten

Im ersten Fall von Konfigurationsbeispielen gehen wir vom Fall einer äußerst einfachen Systemvoraussetzung aus. Es gibt manchmal wirklich das Bestreben, etwas zu kompliziert zu machen, statt so einfach wie möglich mit geringstem Aufwand.

Abschnitt 3.3.1.1 dokumentiert den Servertyp, der vielleicht der richtige für CD-ROM Freigaben ist oder der auf Dokumente für Netzwerk-Benutzer verweist. Diese Konfiguration

wird ebenfalls in Kapitel 8 „Stand-alone-Server“, Abschnitt 8.3.1 erläutert. Der Zweck dieser Konfiguration ist es, ein Freigabe-Laufwerk zur Verfügung zu stellen, auf das von jedem, auch von Gästen, lesend zugegriffen werden kann.

Das zweite Beispiel zeigt eine Minimal-Konfiguration eines Druckservers, so dass jedermann drucken kann, der die richtigen Druckertreiber auf seinem Rechner installiert hat. Dies ist ein Abbild des Systems, das in Kapitel 8 „Stand-alone-Server“, Abschnitt 8.3.2 beschrieben ist.

Das nächste Beispiel ist das eines gesicherten Datei- und Druckservers in einer Büroumgebung, der nur von Benutzern genutzt werden kann, die ein Konto auf diesem System haben. Dieser Server ist absichtlich als ein Arbeitsgruppen-, Datei- und Druckserver ausgelegt, ist aber wesentlich sicherer als ein anonymer Dateiserver. Diese Art von System wird typischerweise die Bedürfnisse eines kleinen Büros abdecken. Der Server bietet keine Netzwerk- Anmelde-Möglichkeiten und keinen Domänencontroller, ist also nur ein Network Attached Storage (NAS)-Device- und Druckserver.

Abschließend betrachten wir noch ein etwas komplexeres System, das sowohl in ein Microsoft Windows-Netzwerk integriert ist als auch dieses komplett ersetzen kann. Die zur Verfügung gestellten Beispiele decken sowohl Domänen-Mitgliedsserver ab als auch Samba-Domänencontroller (PDC/BDC), und schlussendlich beschreiben wir detailliert ein großes verteiltes Netzwerk mit Außenstellen in Filialen.

3.3 Arbeitsbeispiele

Die Konfigurationsbeispiele sind so angelegt, dass sie alles enthalten, um Samba zum Laufen zu bekommen. Sie beinhalten keine grundlegenden Konfigurationen von Betriebsystem-Plattformen, dies würde den Rahmen dieses Texts sprengen.

Es wird des Weiteren davon ausgegangen, dass Samba korrekt installiert wurde, entweder durch Installationspakete, die vom Betriebssystem-Provider zur Verfügung gestellt wurden, oder auf andere Weise.

3.3.1 Stand-alone-Server

Der Begriff „*Stand-alone-Server*“ bedeutet nichts anderes, als die Tatsache, dass es sich nicht um einen Domänencontroller handelt und der Server auch nicht an der Domänenkontrolle teilnimmt. Es kann ein sehr einfacher Arbeitsgruppen-ähnlicher Server sein, oder es kann sich auch um einen etwas komplexeren Server als Mitglied eines Domänensicherheitskontextes handeln.

3.3.1.1 Anonymer Nur-Lese-Dokumenten-Server

Das Ziel dieses Servertyps ist es, jedem Benutzer jedes Dokument oder jede Datei zugänglich zu machen, das bzw. die auf den Freigaberessourcen liegt. Die Freigaberessourcen können dabei ein CD-ROM-Laufwerk, ein CD-ROM-Image oder eine Dateispeicherebene sein.

Als die Beispiele entwickelt wurden, wurde Wert darauf gelegt, dass das System wachsen und mehr Möglichkeiten bieten kann, wie es eben im echten Arbeitsalltag passiert, wenn eine Firma in ihrer Größe und ihren Bedürfnissen wächst und Veränderung braucht.

Die Konfigurationsdatei:

Beispiel 3.3.1. Konfiguration Anonymer Nur-Lese-Server

```
# Global parameters

[global]
        workgroup = MITTELERDE
        netbios name = HOBBIT
        security = share

[data]
        comment = Daten
        path = /export
        read only = Yes
        guest ok = Yes
```

- Der Dateisystem-Freigabepunkt wird `/export` sein.
- Alle Dateien werden von einem Benutzer namens Jack Baumbach gehalten. Jacks Anmeldename wird *jackb* sein. Sein Passwort wird *m0r3pa1n* — sein, natürlich ist das nur das Beispiel, das wir benutzen; benutzen Sie es nicht in einer Produktionsumgebung, da alle Leser dieses Dokuments das Passwort kennen werden.

Installationsprozedur Nur-Lese-Server

1. Fügen Sie den Benutzer dem System hinzu (mit Erzeugung des Benutzer-Homeverzeichnisses):

   ```
   root# useradd -c "Jack Baumbach" -m -g users -p m0r3pa1n jackb
   ```

2. Erzeugen Sie das Verzeichnis, und setzen Sie die Rechte und Mitgliedschaft:

   ```
   root# mkdir /export
   root# chmod u+rwx,g+rx,o+rx /export
   root# chown jackb.users /export
   ```

3. Kopieren Sie die Dateien, die freigegeben werden sollen, nach `/export`.
4. Installieren Sie die Samba-Konfigurationsdatei (`/etc/samba/smb.conf`) wie gezeigt.
5. Testen der Konfigurationsdatei:

   ```
   root# testparm
   ```

Beachten Sie alle Fehlermeldungen, die evtl. angezeigt werden. Fahren Sie nicht fort, bevor Sie nicht eine fehlerfreie Rückmeldung erhalten. Ein Beispiel der Rückmeldungen der folgenden Datei wird die Datei anzeigen.

```
Load smb config files from /etc/samba/smb.conf
Processing section "[data]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
[Press enter]

# Global parameters
[global]
   workgroup = MITTELERDE
   netbios name = HOBBIT
   security = share

[data]
   comment = Data
   path = /export
   read only = Yes
   guest only = Yes
```

6. Starten Sie Samba mit der für Ihr Betriebssystem-Plattform möglichen Methode.
7. Konfigurieren Sie Ihren Microsoft Windows-Client für die Arbeitsgruppe *MITTELERDE*, setzen Sie den Maschinennamen auf ROBBINS, starten Sie den PC neu, und warten Sie ein paar (2 - 5) Minuten. Dann öffnen Sie den Windows Explorer und betrachten die Netzwerkumgebung. Die Maschine HOBBIT sollte sichtbar sein. Wenn Sie auf das Icon dieser Maschine klicken, sollte es sich öffnen und Zugriff auf die Freigabe *data* ermöglichen. Danach klicken Sie auf diese Freigabe, und Sie sollten Zugriff auf die Dateien haben, die wir vorher im `/export` Verzeichnis abgelegt hatten.

Die oben genannten Informationen (die nachstehenden „*global parameters*“) stellen den kompletten Inhalt der Datei `/etc/samba/smb.conf` dar.

3.3.1.2 Anonymer Schreib-Lese-Dokumenten-Server

Sie sollten diese Konfiguration als eine Erweiterung des vorstehenden Beispiels ansehen. Der Unterschied ist, dass der Freigabezugriff nun mit der Benutzeridentität von jackb und der primären Gruppe, der jackb angehört, zusammenhängt. Eine weitere Verbesserung, die wir machen können, ist, den Benutzer *jackb* zu der Datei `smbpasswd` hinzuzufügen. Um dies zu erledigen, machen Sie Folgendes:

```
root# smbpasswd -a jackb
New SMB password: m0r3pa1n
Retype new SMB password: m0r3pa1n
```

```
Added user jackb.
```

Das Hinzufügen dieses Benutzers zu der Datei `smbpasswd` erlaubt es, dass alle Dateien, die in den Explorer-Eigenschaften angezeigt werden, als zu *jackb* gehörend angezeigt werden und nicht mit *Unbekannter Benutzer* beschriftet sind.

Die komplette geänderte Datei `smb.conf` wird in Beispiel 3.3.2 dargestellt.

Beispiel 3.3.2. Geänderte anonyme Schreib-Lese-Datei smb.conf

```
# Globale Parameter

[global]
        workgroup = MITTELERDE
        netbios name = HOBBIT
        security = SHARE

[data]
        comment = Daten
        path = /export
        force user = jackb
        force group = users
        read only = No
        guest ok = Yes
```

3.3.1.3 Anonymer Druckserver

Ein anonymer Druckserver bietet zwei Vorteile:

- Er erlaubt das Drucken auf allen Druckern von einer einzigen Stelle aus.
- Er reduziert den Netzwerkverkehr dadurch, dass viele Benutzer nur eine beschänkte Anzahl von Druckern nutzen können.

Bei der einfachsten Form von anonymen Druckservern ist es allgemein so, dass die korrekte Installation von Druckertreibern auf Windows-Arbeitsstationen verlangt wird. In diesem Fall wird der Druckserver so ausgelegt, dass er Druckaufträge einfach zum Spooler durchreicht, und der Spooler sollte auf „*raw pass-through*“ für den Drucker konfiguriert sein. Mit anderen Worten: Der Drucker-Spooler darf keinen Filter benutzen oder den Datenstrom zum Drucker in irgendeiner Form verarbeiten.

In dieser Konfiguration ist es nicht erwünscht, den Drucker-Wizard anzuzeigen, und wir wollen auch keinen automatischen Treiberdownload haben, also werden wir dies in der folgenden Konfiguration auch abschalten. Beispiel 3.3.3 ist die daraus entstandene Datei `smb.conf`.

Die vorangegangene Konfiguration ist nicht ideal. Sie benutzt keine angenehmen Funktionen und stellt absichtlich keine elegante Lösung dar. Dennoch: Sie ist grundlegend, und sie druckt.

Beispiel 3.3.3. Anonymer Druckserver smb.conf

```
# Globale Parameter

[global]
        workgroup = MITTELERDE
        netbios name = LUTHIEN
        security = share
        printcap name = cups
        disable spoolss = Yes
        show add printer wizard = No
        printing = cups

[printers]
        comment = Alle Drucker
        path = /var/spool/samba
        guest ok = Yes
        printable = Yes
        use client driver = Yes
        browseable = No
```

ANMERKUNG

Windows-Benutzer müssen einen lokalen Drucker installieren und dann die Ausgabeschnittstelle zum Drucker ändern, nachdem sie die Treiber installiert haben. Die Ausgabeschnittstelle kann dann auf den Netzwerkdrucker dieser Maschine gesetzt werden.

Stellen Sie sicher, dass das Verzeichnis `/var/spool/samba` wie gewünscht verwendet werden kann. Die folgenden Schritte stellen dies sicher:

- Das Verzeichnis muss durch den Benutzer superuser (root) und dessen Gruppe gehalten werden:

```
root# chown root.root /var/spool/samba
```

- Die Verzeichnis-Rechte müssen für öffentlichen Lese-Schreibzugriff mit dem sticky-bit wie gezeigt gesetzt werden:

```
root# chmod a+rw TX /var/spool/samba
```

ANMERKUNG

Auf CUPS-aktivierten Systemen gibt es eine Möglichkeit, raw-Daten direkt auf den Drucker auszugeben, ohne diese durch CUPS-Druckerfilter hindurchzuleiten. An Stellen, an denen diese Methode erwünscht ist, muss ein so genanntes raw-printing device konfiguriert sein. Es ist außerdem notwendig, den raw mime-Handler in den Dateien `/etc/mime.conv` und `/etc/mime.types` einzuschalten. Sehen Sie in Abschnitt ?? nach.

3.3.1.4 Sicherer Lese-Schreib-Datei- und Druck-Server

Nach diesem einfachen System sehen wir uns einen etwas komplexeren Server an.

Unser neuer Server wird einen öffentlichen Bereich zur Dateiablage verlangen, der nur von authentifizierten Benutzern (z.B. solchen mit einem lokalen Konto) beschrieben werden kann, und enthält außerdem ein Home-Verzeichnis. Es wird einen Drucker geben, der für alle verfüg- und nutzbar sein wird.

Diese konstruierte Umgebung (es wurde keine Spionage zur Erlangung der Daten durchgeführt) zeigt eine sehr einfache Umgebung, die *sicher genug*, aber nicht zu kompliziert ist.

Die Benutzer werden sein: Jack Baumbach, Mary Orville und Amed Sehkah. Jeder wird ein Passwort haben (diese werden in weiteren Beispielen dann nicht nochmals aufgeführt). Mary wird die Druckeradministratorin sein und wird alle Dateien in dem öffentlichen Bereich halten.

Diese Konfiguration wird auf der *User Level Security* basieren, die den Standard darstellt und die standardmäßig Microsoft Windows-kompatible verschlüsselte Passwörter in einer Datei `/etc/samba/smbpasswd` ablegt. Der Standard-`smb.conf`-Eintrag, der dies ermöglicht, ist: passdb backend = smbpasswd, guest. Da dies der Standard ist, ist es nicht notwendig, ihn in die Konfigurationsdatei zu schreiben. Beachten Sie dabei bitte, dass der Gast-Backend automatisch in die Liste der aktiven passdb-Backends eingetragen wird, egal ob dies in der Samba-Konfigurationsdatei direkt aufgeführt wird oder nicht. Installieren des Secure Office Servers

1. Fügen Sie alle Benutzer zum Betriebssystem hinzu:

```
root# useradd -c "Jack Baumbach" -m -g users -p m0r3pa1n jackb
root# useradd -c "Mary Orville" -m -g users -p secret maryo
root# useradd -c "Amed Sehkah" -m -g users -p secret ameds
```

2. Konfigurieren Sie die Samba-`smb.conf`-Datei, wie in Beispiel 3.3.4 beschrieben.

Beispiel 3.3.4. Secure Office Server smb.conf

```
# Globale Parameter

[global]
        workgroup = MITTELERDE
        netbios name = OLORIN
        printcap name = cups
        disable spoolss = Yes
        show add printer wizard = No
        printing = cups

[homes]
        comment = Home-Verzeichnisse
        valid users = %S
        read only = No
        browseable = No

[public]
        comment = Daten
        path = /export
        force user = maryo
        force group = users
        guest ok = Yes

[printers]
        comment = Alle Drucker
        path = /var/spool/samba
        printer admin = root, maryo
        create mask = 0600
        guest ok = Yes
        printable = Yes
        use client driver = Yes
        browseable = No
```

3. Initialisieren Sie die Microsoft Windows-Passwort-Datenbank mit den neuen Benutzern:

```
root# smbpasswd -a root
New SMB password: bigsecret
Reenter smb password: bigsecret
Added user root.

root# smbpasswd -a jackb
New SMB password: m0r3pa1n
Retype new SMB password: m0r3pa1n
Added user jackb.
```

```
root# smbpasswd -a maryo
New SMB password: secret
Reenter smb password: secret
Added user maryo.

root# smbpasswd -a ameds
New SMB password: mysecret
Reenter smb password: mysecret
Added user ameds.
```

4. Installieren Sie die Drucker, indem Sie das CUPS-Web-Interface nutzen. Stellen Sie sicher, dass alle Drucker, die mit Microsoft Windows-Clients freigegeben sind, als raw printing devices installiert sind.

5. Starten Sie Samba mit dem betriebssystem-eigenen Administrations-Interface. Alternativ können Sie dies auch manuell tun:

```
root#  nmbd; smbd;
```

6. Konfigurieren Sie das `/export`-Verzeicnis:

```
root# mkdir /export
root# chown maryo.users /export
root# chmod u=rwx,g=rwx,o-rwx /export
```

7. Überprüfen Sie, dass Samba korrekt läuft:

```
root# smbclient -L localhost -U%
Domain=[MITTELERDE] OS=[UNIX] Server=[Samba-3.0.0]

Sharename      Type      Comment
---------      ----      -------
public         Disk      Data
IPC$           IPC       IPC Service (Samba-3.0.0)
ADMIN$         IPC       IPC Service (Samba-3.0.0)
hplj4          Printer   hplj4

Server               Comment
---------            -------
OLORIN               Samba-3.0.0

Workgroup            Master
---------            -------
MITTELERDE             OLORIN
```

8. Verbinden Sie sich zu OLORIN als maryo:

```
root# smbclient //olorin/maryo -Umaryo%secret
OS=[UNIX] Server=[Samba-3.0.0]
smb: \> dir
.                           D        0  Sat Jun 21 10:58:16 2003
..                          D        0  Sat Jun 21 10:54:32 2003
Documents                    D        0  Fri Apr 25 13:23:58 2003
DOCWORK                      D        0  Sat Jun 14 15:40:34 2003
OpenOffice.org               D        0  Fri Apr 25 13:55:16 2003
.bashrc                      H     1286  Fri Apr 25 13:23:58 2003
.netscape6                  DH        0  Fri Apr 25 13:55:13 2003
.mozilla                    DH        0  Wed Mar  5 11:50:50 2003
.kermrc                      H      164  Fri Apr 25 13:23:58 2003
.acrobat                    DH        0  Fri Apr 25 15:41:02 2003

      55817 blocks of size 524288. 34725 blocks available
smb: \> q
```

Bis hierher sollten Sie die Konfigurationsgrundlagen mitbekommen haben. Ehrlich, jetzt ist es an der Zeit, etwas komplexere Beispiele kennen zu lernen. Für den Rest dieses Kapitels werden wir die Anleitungen abkürzen, da sie vorher bereits behandelt wurden.

3.3.2 Domänen-Mitgliedsserver

In diesem Abschnitt werden wir uns die einfachstmögliche Serverkonfiguration ausdenken, die man erstellen kann, um ein Vertriebsbüro glücklich zu machen. Seien Sie gewarnt, die Anwender sind Vertriebsleute und haben dementsprechend schlimme Anforderungen. Das Budget sieht nur einen Server für diese Einrichtung vor.

Das Netzwerk wird durch eine interne Information Services Group (ISG) verwaltet, zu der wir gehören. Interne Regeln sind typisch für eine mittelständische Organisation; die Personalabteilung ist der Ansicht, dass die ISG ihr untersteht, weil deren Mitglieder ständig Benutzer hinzufügen oder löschen. Des Weiteren müssen die Abteilungsleiter zähnefletschend darum kämpfen, grundlegende Netzwerkdienste für Ihre Mannschaft zu erhalten. Die Buchhaltung ist natürlich ebenfalls wieder etwas anderes, sie bekommt stets, was sie braucht. Dies sollte vorerst die Situation beschreiben.

Wir werden die Benutzer aus dem letzten Beispiel nehmen. Der Vertrieb hat einen eigenen zentralen Drucker, den alle Abteilungsangehörigen nutzen können. Es gibt auch noch einen Scheckdrucker, den aber nur die Person nutzen darf, die autorisiert ist, Schecks zu drucken. Der Chefbuchhalter (CFO) möchte, dass dieser Drucker vollständig geschützt ist und deshalb auch in seinem eigenen privaten Teil des Büros aufgebaut ist. Deshalb muss es ein Netzwerkdrucker sein.

Die Vertriebsstelle benutzt eine Vertriebssoftware namens *SpytFull*, die von einem zentralen Applikationsserver aus läuft. Die Software ist für einen Server lizenziert, es gibt keine

Arbeitsplatzkomponenten, und sie wird von einer gemappten Freigabe aus gestartet. Die Datenablage erfolgt in einem Unix-basierenden SQL-Backend. Die UNIX-Gurus kümmern sich darum, es ist also nicht unser Problem.

Die Vertriebsmanagerin (maryo) möchte ein allgemein zugängliches Dateisystem und zusätzlich eine getrennte Dateiablage für Formbriefe (nastygrams). Der Bereich für die Formbriefe soll für alle Vertriebsmitarbeiter außer der Managerin selbst nur lesbar sein. Das allgemein zugängliche Dateisystem muss ein strukturiertes Layout haben: Es muss sowohl einen zentralen Bereich für alle Mitarbeiter geben, um allgemeine Dokumente zu speichern, als auch einen getrennten Bereich für den jeweiligen Mitarbeiter selbst, in dem er private Dinge ablegen kann, aber die Managerin möchte auf alle diese Bereiche vollen Zugriff haben. Die Benutzer haben ein privates Home-Verzeichnis für persönliche Dateien, die arbeitsgebunden sind, und für Materialien, die nichts mit ihrer Arbeit zu tun haben.

3.3.2.1 Beispielkonfiguration

Der Server *valinor* wird ein Mitglied der Firmendomäne sein. Die Vetriebsleute haben nur einen lokalen Server. Benutzerkonten werden auf dem Domänencontroller liegen, genauso wie die Arbeitsplatzprofile und alle Netzwerk-Richtliniendateien.

1. Fügen Sie keine Benutzer zu den UNIX/Linux-Servern hinzu, dies wird in der zentralen Domäne gemacht.
2. Konfigurieren Sie `smb.conf`, wie in Beispiel 3.3.5 und Beispiel 3.3.6 beschrieben.

Beispiel 3.3.5. Mitgliedsserver smb.conf (globale Einstellungen)

```
# Globale Parameter

[global]
        workgroup = MITTELERDE
        netbios name = VALINOR
        security = DOMAIN
        printcap name = cups
        disable spoolss = Yes
        show add printer wizard = No
        idmap uid = 15000-20000
        idmap gid = 15000-20000
        winbind separator = +
        winbind use default domain = Yes
        use sendfile = Yes
        printing = cups
```

3. Treten Sie der Domäne bei. Beachten Sie: Starten Sie Samba nicht, bevor dieser Schritt abgeschlossen ist!

```
root# net rpc join -Uroot%'bigsecret'
```

Beispiel 3.3.6. Mitglieds-Server smb.conf (Freigaben und Dienste)

```
[homes]
       comment = Home-Verzeichnisse
       valid users = %S
       read only = No
       browseable = No

[spytfull]
       comment = Nur für Vertriebsanwendungen
       path = /export/spytfull
       valid users = @Accounts
       admin users = maryo
       read only = Yes

[public]
       comment = Daten
       path = /export/public
       read only = No

[printers]
       comment = Alle Drucker
       path = /var/spool/samba
       printer admin = root, maryo
       create mask = 0600
       guest ok = Yes
       printable = Yes
       use client driver = Yes
       browseable = No
```

```
Joined domain MITTELERDE.
```

4. Stellen Sie unbedingt sicher, dass der **nscd**-Daemon auf allen Systemen abgeschaltet oder heruntergefahren ist, auf denen **winbind** lauffähig konfiguriert ist.

5. Starten Sie Samba mit der für Ihre Betriebssystem-Plattform vorgegebenen Methode. Sie können dies als root auch manuell ausführen:

```
root# nmbd; smbd; winbindd;
```

6. Konfigurieren Sie die Nameservice-Switch-Konfigurationsdatei auf Ihrem System, um Benutzer- und Gruppennamen durch winbind aufzulösen. Ändern Sie die folgenden Zeilen in `/etc/nsswitch.conf`:

```
passwd: files winbind
```

```
group:  files winbind
hosts:  files dns winbind
```

7. Setzen Sie das Passwort, um **wbinfo** nutzen zu können:

```
root# wbinfo --set-auth-user=root%'bigsecret'
```

8. Überprüfen Sie, dass die Domänenbenutzer und Gruppenzugehörigkeiten korrekt aufgelöst werden können, indem Sie das Folgende ausführen:

```
root# wbinfo -u
MITTELERDE+maryo
MITTELERDE+jackb
MITTELERDE+ameds
...
MITTELERDE+root

root# wbinfo -g
MITTELERDE+Domain Users
MITTELERDE+Domain Admins
MITTELERDE+Domain Guests
...
MITTELERDE+Accounts
```

9. Überprüfen Sie, dass **winbind** läuft. Das Folgende demonstriert die korrekte Auflösung des Benutzernamens durch das System-Dienstprogramm **getent**:

```
root# getent passwd maryo
maryo:x:15000:15003:Mary Orville:/home/MITTELERDE/maryo:/bin/false
```

10. Ein abschließender Test, ob wir dies auch unter Kontrolle haben, versichert uns dann:

```
root# touch /export/a_file
root# chown maryo /export/a_file
root# ls -al /export/a_file
...
-rw-r--r--    1 maryo    users       11234 Jun 21 15:32 a_file
...

root# rm /export/a_file
```

11. Die Konfiguration ist nahezu fertig. Dies ist ein günstiger Zeitpunkt, um die Verzeichnisstruktur für diese Einrichtung anzulegen:

```
root# mkdir -p /export/{spytfull,public}
root# chmod ug=rwxS,o=x /export/{spytfull,public}
root# chown maryo.Accounts /export/{spytfull,public}
```

3.3.3 Domänencontroller

Für den Rest dieses Kapitels liegt der Schwerpunkt auf der Konfiguration der Domänenkontrolle. Die folgenden Beispiele sind für zwei Implementierungsstrategien ausgelegt. Erinnern Sie sich: Unsere Aufgabe ist eine einfache, aber funktionierende Lösung. Der Rest dieses Buches soll helfen, die Gelegenheit für eine größere Funktionalität und die damit einhergehende Komplexität zu beleuchten.

Sie können einen Domänencontroller recht einfach konfigurieren, indem Sie das neue tdbsam-Passwort-Backend nutzen. Dieser Konfigurationstyp ist gut für kleine Büros, hat aber eine beschränkte Skalierungsmöglichkeit (Replikation funktioniert nicht), und die Performance wird vermutlich sinken, wenn die Größe und Komplexität der Domäne zunehmen.

Die Nutzung von tdbsam sollte am besten auf Einrichtungen beschränkt werden, die nicht mehr als einen primären Domänencontroller (PDC) benötigen. Wenn die Größe einer Domäne anwächst, kommt der Wunsch nach einem zusätzlichen Domänencontroller auf. Versuchen Sie nicht, eine Microsoft Windows-Netzwerkumgebung zu klein auszulegen; Domänencontroller stellen lebenswichtige Authentifizierungsdienste zur Verfügung. Die folgenden Merkmale sind Symptome einer zu klein ausgelegten Domänencontroller-Umgebung:

- Domänen-Anmeldungen schlagen sporadisch fehl.
- Dateizugriffe auf einen Domänen-Mitgliedsserver schlagen sporadisch fehl, es kommt zu Fehlermeldungen mit Zugriffsverweigerungen.

Eine besser skalierbare Option für Domänencontroller-Authentifizierungs-Backends könnte das Microsoft Active Directory oder ein LDAP-basierendes Backend nutzen. Samba-3 stellt dies für beide Optionen als einen Domänen-Mitgliedsserver zur Verfügung. Als ein PDC ist Samba-3 nicht in der Lage, eine genaue Alternative zu den Funktionalitäten zur Verfügung zu stellen, die Active Directory bietet. Samba-3 kann eine skalierbare LDAP-basierende PDC/BDC-Lösung zur Verfügung stellen.

Das tdbsam-Authentifizierungs-Backend bietet keine Funktion zum Replizieren der Datenbankinhalte, außer für externe Möglichkeiten (z.B. gibt es kein autarkes Protokoll in Samba-3 für die Security-Account-Manager-(SAM-)Datenbank-Replikation).

Anmerkung

Falls Sie also mehr als einen Domänencontroller benötigen, sollten Sie kein tdbsam-Authentifizierungs-Backend benutzen.

3.3.3.1 Beispiel: Ingenieur-Büro

Der Netzwerkserver des Ingenieurbüros, den wir hier präsentieren, ist dazu gedacht, das neue tdbsam-Passwort-Backend zu demonstrieren. Die tdbsam-Funktion ist neu in Samba-3. Sie soll viele Benutzer- und Maschinenkonten zur Verfügung stellen, die mit Microsoft Windows NT4 möglich sind. Es ist sicher, dies in kleineren Netzwerken zu benutzen.

1. Eine PDC-Konfiguration in Produktion, die das tdbsam-Passwort-Backend benutzt, können Sie Beispiel 3.3.8 hier sehen Beispiel 3.3.8:

Beispiel 3.3.7. Ingenieurbüro smb.conf (Globale Einstellungen)

```
[global]
        workgroup = MITTELERDE
        netbios name = FRODO
        passdb backend = tdbsam
        printcap name = cups
        add user script = /usr/sbin/useradd -m %u
        delete user script = /usr/sbin/userdel -r %u
        add group script = /usr/sbin/groupadd %g
        delete group script = /usr/sbin/groupdel %g
        add user to group script = /usr/sbin/usermod -G %g %u
        add machine script = /usr/sbin/useradd -s /bin/false \
-d /dev/null %u
# Hinweis: Das Folgende spezifiziert das Standard-Logon-Skript.
# Pro-Benutzer-Logon-Skripten können im Benutzerkonto spezifiziert werden, und zwar durch pdbed
        logon script = scripts\logon.bat
# Dies setzt den Standard-Profilpfad. Setzen Sie Pro-Benutzerpfade mit pdbedit
        logon path = \\%L\Profiles\%U
        logon drive = H:
        logon home = \\%L\%U
        domain logons = Yes
        os level = 35
        preferred master = Yes
        domain master = Yes
        idmap uid = 15000-20000
        idmap gid = 15000-20000
        printing = cups
```

---

2. Erstellen Sie die benötigten UNIX-Gruppenkonten mit Ihrem betriebssystem-spezifischen Werkzeug:

```
root# groupadd ntadmins
root# groupadd designers
root# groupadd engineers
root# groupadd qateam
```

3. Erstellen Sie Benutzerkonten auf dem System mit Ihrem betriebssystem-spezifischen Werkzeug. Stellen Sie sicher, dass die Benutzer-Home-Verzeichnisse ebenfalls erzeugt wurden. Fügen Sie den Gruppen die Benutzer zu, die Sie für die Zugriffskontrolle auf die Dateien, Verzeichnisse und Drucker, wie in Ihrer Samba-Umgebung gewünscht, benötigen.

4. Weisen Sie jeder UNIX-Gruppe die NT-Gruppe zu: (Vielleicht ist es hilfreich, diesen Text in ein kleines Shell-Skript namens `initGroups.sh` zu kopieren.) Shell-Skript zur Initialisierung der Gruppen-Zuweisungen

```
#!/bin/bash
#### Shell-Skript für spätere Verwendung aufbewahren

# Als Erstes weisen wir bekannte Gruppen zu:
net groupmap modify ntgroup="Domain Admins" unixgroup=ntadmins rid=512
net groupmap modify ntgroup="Domain Users"  unixgroup=users    rid=513
net groupmap modify ntgroup="Domain Guests" unixgroup=nobody   rid=514

# Dann für unsere eigenen Domänen-Gruppen:
net groupmap add ntgroup="Designers" unixgroup=designers type=d rid=1112
net groupmap add ntgroup="Engineers" unixgroup=engineers type=d rid=1113
net groupmap add ntgroup="QA Team"   unixgroup=qateam    type=d rid=1114
```

5. Erzeugen Sie das Verzeichnis `scripts` zur Nutzung in der *[NETLOGON]*-Freigabe:

```
root# mkdir -p /var/lib/samba/netlogon/scripts
```

   Legen Sie die Anmelde-Skripten (Batch- oder cmd-Skripten), die verwendet werden sollen, in diesem Verzeichnis ab.

Die vorige Konfiguration stellt einen voll funktionierenden primären Domänencontroller (PDC) zur Verfügung, zu dem noch die gewünschten Dateifreigaben und Drucker hinzugefügt werden müssen.

3.3.3.2 Eine große Organisation

In diesem Kapitel wollen wir kurz einen Überblick über eine Samba-3-Konfiguration geben, die ein Authentifizierungs-Backend nutzt, das auf dem Lightweight Directory Access Protocol (LDAP) basiert. Die Hauptgründe für diese Wahl waren zum einem die Möglichkeit, einen primären und einen Backup-Domänencontroller (BDC) zur Verfügung zu stellen, und zum anderen ein größeres Maß an Skalierbarkeit, um den Anforderungen an eine sehr verteilte Umgebung gerecht zu werden.

Der primäre Domänencontroller Dies ist ein Beispiel für eine Minimalkonfiguration, um einen Samba-3-PDC mit einem LDAP-Authentifizierungs-Backend zu nutzen. Es wird vorausgesetzt, dass das Betriebssystem korrekt konfiguriert wurde.

Die Idealx-Skripten (oder gleichwertige) werden benötigt, um LDAP-basierende Posix- und/oder SambaSamAccounts zu verwalten. Die Idealx-Skripten können von dieser Idealx <http://www.idealx.org>-Webseite heruntergeladen werden. Sie können ebenfalls vom Samba-tarball genommen werden. Linux-Distributionen installieren die Idealx-Skripten meist in dem Verzeichnis `/usr/share/doc/packages/sambaXXXXXX/examples/LDAP/smbldap-tools`. Die Idealx-Skriptversionen `smbldap-tools-0.8.2` sind bekanntermaßen eine gute Arbeitsgrundlage.

1. Nehmen Sie aus den Samba-Quellen `~/examples/LDAP/samba.schema`, und kopieren Sie dies in das Verzeichnis `/etc/openldap/schema/`.

2. Setzen Sie den LDAP-Server auf. Dieses Beispiel passt zu OpenLDAP 2.1.x. Die Datei `/etc/openldap/slapd.conf` sieht so aus: Beispieldatei slapd.conf

```
# Hinweis: auskommentierte Zeilen wurden entfernt
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/samba.schema

pidfile         /var/run/slapd/slapd.pid
argsfile        /var/run/slapd/slapd.args

database        bdb
suffix          "dc=quenya,dc=org"
rootdn          "cn=Manager,dc=quenya,dc=org"
rootpw          {SSHA}06qDkonA8hk6W6SSnRzWj0/pBcU3m0/P
# Das obige Passwort ist 'nastyon3'

directory     /var/lib/ldap

index   objectClass     eq
index cn                        pres,sub,eq
index sn                        pres,sub,eq
index uid                       pres,sub,eq
index displayName               pres,sub,eq
index uidNumber                 eq
index gidNumber                 eq
index memberUid                 eq
index   sambaSID                eq
index   sambaPrimaryGroupSID    eq
index   sambaDomainName         eq
index   default                 sub
```

3. Erzeugen Sie die folgende Datei `samba-ldap-init.ldif`:

```
# Organisation für SambaXP Demo
dn: dc=quenya,dc=org
objectclass: dcObject
objectclass: organization
dc: quenya
o: SambaXP Demo
description: Der SambaXP Demo LDAP Tree

# Organisatorische Rolle für die Verwaltung des Verzeichnisses
dn: cn=Manager,dc=quenya,dc=org
objectclass: organizationalRole
cn: Manager
description: Directory Manager

# Aufsetzen der Container für die Benutzer
dn: ou=People, dc=quenya, dc=org
objectclass: top
objectclass: organizationalUnit
ou: People

# Aufsetzen eines Administrator-Handles für die People OU
dn: cn=admin, ou=People, dc=quenya, dc=org
cn: admin
objectclass: top
objectclass: organizationalRole
objectclass: simpleSecurityObject
userPassword: {SSHA}0jBHgQ1vp4EDX2rEMMfIudvRMJoGwjVb
# Das vorige Passwort ist 'mordonL8'
```

4. Laden Sie die vorigen Initialdaten in die LDAP-Datenbank:

```
root# slapadd -v -l initdb.ldif
```

5. Starten Sie den LDAP-Server durch das Werkzeug oder die Methode, das bzw. die für die verwendete Betriebssystem-Plattform am besten geeignet ist.

6. Installieren Sie die Idealx-Skriptdateien im Verzeichnis `/usr/local/sbin`, und konfigurieren Sie dann die Datei `smbldap_conf.pm`, um Ihre Systemkonfiguration anzupassen.

7. Die Datei `smb.conf`, die diesen Backend steuert, kann hier gefunden werden Beispiel 3.3.9:

8. Fügen Sie das LDAP-Passwort zu der Datei `secrets.tdb` hinzu, so dass Samba die LDAP-Datenbank aktualisieren kann:

```
root# smbpasswd -w mordonL8
```

9. Fügen Sie Benutzer und Gruppen wie benötigt hinzu. Benutzer und Gruppen, die über Samba-Werkzeuge hinzugefügt wurden, werden automatisch sowohl dem LDAP-Backend als auch dem Betriebssystem hinzugefügt.

Backup-Domänencontroller Beispiel 3.3.10 zeigt die Beispielkonfiguration für den BDC.

1. Entscheiden Sie, ob der BDC seinen eigenen LDAP-Server haben soll oder nicht. Falls der BDC auch der LDAP-Server ist, ändern Sie die folgende `smb.conf` wie angezeigt. Die Standardkonfiguration in Beispiel 3.3.10 benutzt einen zentralen LDAP-Server.
2. Konfigurieren Sie die Verzeichnisse NETLOGON und PROFILES für den PDC wie in Beispiel 3.3.10.

Beispiel 3.3.8. Ingenieurbüro smb.conf (Freigaben und Dienste)

```
[homes]
       comment = Home-Verzeichnisse
       valid users = %S
       read only = No
       browseable = No
# Drucker Auto-Freigabe (stellt Drucker durch CUPS zur Verfügung)

[printers]
       comment = Alle Drucker
       path = /var/spool/samba
       printer admin = root, maryo
       create mask = 0600
       guest ok = Yes
       printable = Yes
       browseable = No

[print$]
       comment = Druckertreiber-Freigabe
       path = /var/lib/samba/drivers
       write list = maryo, root
       printer admin = maryo, root
# Wird für Domänen-Anmeldungen benötigt

[netlogon]
       comment = Netzwerk-Anmeldedienst
       path = /var/lib/samba/netlogon
       admin users = root, maryo
       guest ok = Yes
       browseable = No
# Für Profile, erstellt ein Benutzerverzeichnis unterhalb des Pfades
# z.B.: mkdir -p /var/lib/samba/profiles/maryo

[Profiles]
       comment = Roaming Profile Share (wandernde Benutzerprofile)
       path = /var/lib/samba/profiles
       read only = No
       profile acls = Yes
# Andere Ressourcen (Freigaben/Drucker) folgen weiter unten.
...
```

Beispiel 3.3.9. LDAP-Backend smb.conf für einen PDC

```
# Globale Parameter

[global]
        workgroup = MITTELERDE
        netbios name = FRODO
        passdb backend = ldapsam:ldap://localhost
        username map = /etc/samba/smbusers
        printcap name = cups
        add user script = /usr/local/sbin/smbldap-useradd.pl -m '%u'
        delete user script = /usr/local/sbin/smbldap-userdel.pl %u
        add group script = /usr/local/sbin/smbldap-groupadd.pl -p '%g'
        delete group script = /usr/local/sbin/smbldap-groupdel.pl '%g'
        add user to group script = /usr/local/sbin/ \
smbldap-groupmod.pl -m '%g' '%u'
        delete user from group script = /usr/local/sbin/ \
smbldap-groupmod.pl -x '%g' '%u'
        set primary group script = /usr/local/sbin/ \
smbldap-usermod.pl -g '%g' '%u'
        add machine script = /usr/local/sbin/smbldap-useradd.pl -w '%u'
        logon script = scripts\logon.bat
        logon path = \\%L\Profiles\%U
        logon drive = H:
        logon home = \\%L\%U
        domain logons = Yes
        os level = 35
        preferred master = Yes
        domain master = Yes
        ldap suffix = dc=quenya,dc=org
        ldap machine suffix = ou=People
        ldap user suffix = ou=People
        ldap group suffix = ou=People
        ldap idmap suffix = ou=People
        ldap admin dn = cn=Manager
        ldap ssl = no
        ldap passwd sync = Yes
        idmap uid = 15000-20000
        idmap gid = 15000-20000
        winbind separator = +
        printing = cups
...
```

Beispiel 3.3.10. Remote LDAP-BDC smb.conf

```
# Globale Parameter

[global]
        workgroup = MITTELERDE
        netbios name = GANDALF
        passdb backend = ldapsam:ldap://frodo.quenya.org
        username map = /etc/samba/smbusers
        printcap name = cups
        logon script = scripts\logon.bat
        logon path = \\%L\Profiles\%U
        logon drive = H:
        logon home = \\%L\%U
        domain logons = Yes
        os level = 33
        preferred master = Yes
        domain master = No
        ldap suffix = dc=quenya,dc=org
        ldap machine suffix = ou=People
        ldap user suffix = ou=People
        ldap group suffix = ou=People
        ldap idmap suffix = ou=People
        ldap admin dn = cn=Manager
        ldap ssl = no
        ldap passwd sync = Yes
        idmap uid = 15000-20000
        idmap gid = 15000-20000
        winbind separator = +
        printing = cups
...
```

Teil II

Basiswissen zur Server-Konfiguration

ERSTE SCHRITTE BEI DER KONFIGURATION

Samba kann in verschiedenen Modi in SMB-Netzwerken operieren. Dieser HOWTO-Abschnitt beinhaltet Informationen darüber, wie Samba unter Berücksichtigung ihrer Netzwerkanforderungen einzurichten ist. Bitte lesen Sie dies aufmerksam durch.

Kapitel 4

SERVER-ARTEN UND SICHERHEITSMODI

Dieses Kapitel enthält Informationen zu den verschiedenen Server-Typen, die Sie im Samba-Server einstellen können. Ein Microsoft-Netzwerk-Administrator, der zu Samba migrieren bzw. Samba nutzen möchte, ist bestimmt interessiert daran, welche Samba-Konfigurationen er vornehmen muss, verglichen mit den Konfigurationen eines Windows-Servers. Es ist wichtig, die Sicherheitsdefinitionen festzulegen, bevor man den Server selbst konfiguriert.

Dieses Kapitel gibt Ihnen einen Überblick über die Sicherheitsmodi von Samba und zeigt, wie sie sich zu denen von Windows verhalten.

Eine Frage, die häufig gestellt wird, lautet: „*Warum will ich Samba nutzen?*“ Die meisten Kapitel enthalten einen Abschnitt, die die positiven Merkmale und Vorteile hervorhebt. Wir hoffen, dass diese Informationen Ihnen diese Frage beantworten können. Wir wollen fair und vernünftig bleiben, denken Sie also daran, dass nicht alle Features für Samba sprechen. Der Vorteil könnte auf unserer Seite sein.

4.1 Positive Merkmale und Vorteile

Zwei Männer gehen eine staubige Straße entlang, als der eine plötzlich einen kleinen roten Stein lostritt. Der Stein setzt sich in seine Sandale und verletzt den Mann am Zeh. Der Mann nimmt den Stein unter zornigem Fluchen aus der Sandale und ist sehr verärgert. Der andere Mann schaut sich den Stein an und sagt: „*Dies ist ein Granat, ich könnte ihn zu Schmuck verarbeiten, und eines Tages wird er einer Prinzessin viel Freude bereiten.*“

Und die Moral von dieser Geschichte: Zwei Männer, zwei verschiedene Betrachtungsweisen des gleichen Steins. Mögen oder hassen. Samba ist wie dieser Stein. Behandeln Sie es richtig, so kann es Ihnen einen großen Dienst erweisen, aber wenn Sie gezwungen sind, Samba zu benutzen, ohne seine Geheimnisse zu kennen, kann es eine Quelle des Unbehagens sein.

Samba startete als Projekt, mit dem die Zusammenarbeit von MS Windows 3.x Clients und Unix-Servern gewährleistet werden sollte. Es ist seit den Anfängen stark gewachsen und stellt jetzt Merkmale und Funktionen zur Verfügung, die es für große Aufgaben geeignet macht. Es hat aber auch ein paar Nachteile, die wir in Abschnitten wie diesem besprechen möchten.

Also, was sind die Vorteile und Merkmale, die wir in diesem Kapitel erwähnen?

- Samba 3 kann einen MS Windows NT4-Domänencontroller ersetzen.
- Samba 3 bietet eine exzellente Kompatibilität mit MS Windows NT4-Domänen und mit nativen Microsoft Active-Directory-Domänen.
- Samba 3 erlaubt volle Interdomain Trusts im NT4-Style.
- Samba hat Sicherheitsmodi, die eine anpassungsfähigere Benutzer-Authentifikation durchführen können als Windows NT4-Domänencontroller.
- Samba 3 unterstützt die parallele Nutzung von verschiedenen Account-Datenbanken.
- Die Account- bzw. Passwort-Datenbanken können mit verschiedenen Methoden verteilt und repliziert werden. Dies ermöglicht mit Samba 3 eine größere Flexibilität als mit MS Windows NT4 - und stellt in vielen Fällen auch ein wesentlich besseres Werkzeug als Active-Directory- Domänen unter Windows 200x dar.

4.2 Server-Arten

Administratoren von Microsoft-Netzwerken beziehen sich oft auf drei verschiedene Server-Arten:

- Domänencontroller
  - Primäre Domänencontroller
  - Backup-Domänencontroller
  - ADS-Domänencontroller
- Domänen-Mitgliedsserver
  - Active-Directory-Domänenserver
  - Domänenserver im NT4-Stil
- Stand-alone-Server

Die Kapitel über Domänencontroller, Backup-Domänencontroller und Domänen-Mitgliedschaft enthalten nützliche Informationen zur Samba-Konfiguration für jede dieser Serverrollen. Wir möchten Sie ermutigen, sich mit diesen Informationen vertraut zu machen.

4.3 Samba-Sicherheitsmodi

In diesem Abschnitt werden die Funktionen und Zwecke der Samba-Sicherheitsmodi beschrieben. Es ist wichtig zu verstehen, wie jede der Sicherheitsmöglichkeiten, die Samba bietet, arbeitet und wie die Windows-Clients konfiguriert werden müssen, damit Sicherheit und Funktionstüchtigkeit gewährleistet sind.

In der SMB/CIFS-Netzwerkwelt gibt es nur zwei Arten der Sicherheit: *User Level* und *Share Level*. Wir bezeichnen diese beiden Arten kollektiv als *Sicherheits- Level*. Durch Realisierung

dieser beiden Security-Level bietet Samba Flexibilitäten, die nicht in Microsoft NT4/200x-Servern vorgesehen sind. Derzeit unterstützt Samba die *Share Level*-Sicherheit nur in einer Richtung, dafür aber vier Arten der *User Level*-Sicherheit. Zusammen gesehen nennen wir die Samba-Sicherheiten *Sicherheitsmodi*. Sie sind bekannt als: *SHARE*-, *USER*-, *DOMAIN*-, *ADS*- und *SERVER*-Modi, und werden in diesem Kapitel behandelt.

Ein SMB-Server sagt dem Client während des Startens, mit welcher Sicherheitsstufe der SMB-Server läuft. Hierbei gibt es zwei Optionen: Share Level und User Level. Diese beiden Optionen beeinflussen die Art, wie der Client sich selbst authentifiziert. Sie beeinflussen nicht direkt die Art, wie der Samba-Server die Sicherheit handhabt. Das klingt ein wenig merkwürdig, aber es passt zu der Weise, wie SMB arbeitet. Bei SMB wird alles vom Client initiiert und kontrolliert, und der Server teilt dem Client nur mit, was verfügbar bzw. erlaubt ist.

4.3.1 User Level-Sicherheit

Der Einfachheit halber möchten wir zuerst die User Level-Sicherheit erläutern. In dieser Sicherheitsstufe sendet der Client einen Session Setup Request und direkt darauf folgend eine Protokoll-Absprache. Diese Anfrage liefert einen Benutzernamen und ein Passwort. Der Server akzeptiert die Benutzernamen/Passwort-Kombination entweder, oder er verweigert sie. An diesem Punkt hat der Server keine Ahnung, welche Freigabe der Client eventuell aufrufen wollte, es wird nur durch folgende Punkte eine Entscheidung für die *Annahme* oder die *Verweigerung* getroffen:

1. Durch den Benutzernamen/das Passwort
2. Durch den Namen des Client-PCs

Wenn der Server den Benutzernamen mit dem entsprechenden Passwort akzeptiert, erwartet der Client, Freigaben einzubinden (unter Verwendung einer *Baum- Verbindung*), ohne ein weiteres Mal das Passwort zu nennen. Der Client geht davon aus, dass alle Zugriffsrechte durch den Benutzernamen/das Passwort aus dem *Session Setup* geregelt werden.

Es ist ebenfalls möglich, dass ein Client verschiedene *Session Setup*-Anfragen sendet. Wenn der Server darauf antwortet, vergibt er an den Client eine *uid* als Authentifizierungsetikett. Der Client kann somit verschiedene Authentifizierungskontexte aufrechterhalten (WinDD, zum Beispiel, ist eine Applikation, die diese Verfahrensweise nutzt).

4.3.1.1 Beispielkonfiguration

Der `smb.conf`-Parameter, der die Sicherheit auf „*User Level*“ setzt, lautet:

```
security = user
```

Dies ist die Standard-Einstellung seit Samba-2.2.x.

4.3.2 Share Level-Sicherheit

Bei der Share Level-Sicherheit authentifiziert sich der Client selbst bei jedem Aufruf einer Freigabe mit einem Passwort. Es wird nicht explizit ein Benutzername vom Client zum

Server gesendet. Der Client erwartet ein Passwort, das mit jeder Freigabe verbunden wird; somit hat Samba die Aufgabe herauszufinden, welchen Benutzernamen der Client verwenden möchte. Einige kommerzielle SMB-Server wie NT assoziieren Passwörter bei der Share Level-Sicherheit direkt mit Freigaben; Samba arbeitet im Gegensatz dazu mit dem UNIX-Authentifizierungsschema, das ein Benutzer/Passwort- Paar statt eines Share/Passwort-Paars erwartet.

Um die Parallele zum MS-Windows-Netzwerk zu verstehen, sollte man in der Begrifflichkeit von Windows 9x/Me denken, wo jemand einen gemeinsam genutzten Ordner freigeben kann, der Nur-Lese- oder Voll-Zugriff mit oder ohne Passwort gestattet.

Viele Clients senden ein Session Setup auch dann, wenn der Server mit Share Level-Sicherheit läuft. Sie übergeben normalerweise einen gültigen Benutzernamen, den sich Samba in einer Liste der möglichen Benutzernamen merkt. Wenn nun der Client eine Verbindung zu einem Freigabe-Baum herstellt, nimmt der Samba-Server den Namen der Freigabe in seine Liste auf (nützlich für Freigaben des Heimat-Verzeichnisses), und jeder Benutzer des user Parameters in der `smb.conf` wird mit dem gesendeten Passwort überprüft. Wenn nun eine Übereinstimmung des anfänglich gesendeten Benutzernamens mit dem für das Share gesendeten Passwort gefunden wird, ist der Client berechtigt, auf dieses Share zuzugreifen.

4.3.2.1 Beispielkonfiguration

Der `smb.conf`-Parameter, der die Sicherheitsstufe auf Share Level-Sicherheit setzt, sieht so aus:

```
security = share
```

Es gibt Berichte, dass neue MS Windows-Clients nicht mit Servern arbeiten möchten, die im Share Level-Sicherheitsmodus laufen. Wir möchten ausdrücklich davor warnen, im Share Level-Modus zu arbeiten.

4.3.3 Domänen-Sicherheitsmodus (User Level Security)

Wenn Samba im security = domain-Modus betrieben wird, hat der Server einen Trust Account (Maschinen-Account) und reicht alle Authentifizierungsanfragen an die Domänencontroller weiter. Mit anderen Worten: Diese Konfiguration macht den Samba-Server zu einem Domänen-Mitglied.

4.3.3.1 Beispielkonfiguration

Samba als Domänen-Mitgliedsserver

Diese Art, den Server zu betreiben, erfordert folgende Parameter in der `smb.conf`:

```
security = domain
workgroup = MITTELERDE
```

Damit dies funktioniert, müssen folgende Schritte untergenommen werden:

1. Richten Sie einen Maschinen-Account für den Samba-Server ein. Benutzen Sie dafür den Server Manager.

2. Auf dem UNIX/Linux-System führen Sie Folgendes aus:

```
root# net rpc join -U administrator%password
```

ANMERKUNG

Samba-2.2.4 und spätere Versionen können durch das Ausführen von folgendem Befehl automatisch einer NT4-Domäne beitreten:

```
root# smbpasswd -j DOMÄNEN-NAMEN -r PDC_NAME \
    -U Administrator%password
```

Samba 3 kann das Gleiche mit folgendem Kommando:

```
root# net rpc join -U Administrator%password
```

Mit Samba 3 ist es nicht nötig, den *DOMÄNEN-NAMEN* oder den *PDC_NAME* anzugeben, da Samba 3 sich diese Informationen aus der `smb.conf` holt.

Um diese Art der Authentifikation zu nutzen, benötigt man einen Standard-UNIX-Account, damit für jeden User eine gültige UNIX-UserID existiert, die vom entfernten Windows-Domänencontroller authentifiziert werden kann. Es spricht allerdings nichts dagegen, dass es diesem UNIX-Account verboten wird, sich einzuloggen, was bei MS Windows nicht möglich ist. Um einen solchen UNIX-Account zu blocken, setzen Sie eine nicht login-fähige Shell in der `/etc/passwd` (z.B. /bin/false als Shell).

Eine Alternative zum Assoziieren von UIDs zu Windows-Usern mit einem Samba-Mitgliedsserver wird in Kapitel Winbind beschrieben.

Für weitere Informationen zur Domänen-Mitgliedschaft lesen Sie bitte das Kapitel Domänen-Mitgliedschaft.

4.3.4 ADS-Sicherheitsmodus (User Level Security)

Sowohl Samba 2.2 als auch Samba 3 können einer ADS-Domäne beitreten. Der Betriebsmodus der Domäne ist für Samba dafür nicht relevant. Beachten Sie, dass Samba 2.2 sowie frühe Versionen von Samba 3.0 nicht einer Domäne mit einem unmodifizierten Windows Server-2003-Domänencontroller beitreten können, da dieser in seiner Voreinstellung das SMB-Signing voraussetzt. Seit Samba 3.0.3 wird dies jedoch unterstützt.

Wenn Sie ADS benutzen und mit Samba 3 starten, können Sie der ADS als normales Active-Directory-Mitglied beitreten. Warum Sie das tun sollten? Ihre Sicherheitsrichtlinien könnten die NT-kompatiblen Authentifizierungsprotokolle schlichtweg verweigern. Wenn

alle Server in Ihrem Netzwerk Windows 2000 und höher nutzen, würde Samba als NT4-artiges Domänen-Mitglied NT-kompatible Authentifizierungsdaten benötigen. Samba im AD-Mitgliedsmodus allerdings kann auch Kerberos-Tickets auswerten.

4.3.4.1 Beispielkonfiguration

```
realm = YOUR.KERBEROS.REALM
security = ADS
```

Für weitere Informationen zu dieser Konfigurationsoption lesen Sie bitte unter Domänen-Mitglied und ADS-Mitglied weiter.

4.3.5 Server Security (User Level Security)

Der Server-Security-Modus ist noch aus den Zeiten übrig geblieben, in denen Samba nicht als Domänen-Mitglied betrieben werden konnte. Sie sollten diesen Modus nicht verwenden, da er viele Nachteile mit sich bringt. Zum Beispiel:

- Potenzielle Account-Sperren auf MS Windows NT4/200x Passwort-Servern.
- Eine Sicherheitslücke, die dazu führt, dass der Passwortserver, der konfiguriert ist, nicht der ist, den man wirklich nutzen möchte.
- Der Modus funktioniert nicht mit Winbind, was nötig ist, um Profile auf entfernten Systemen zu speichern.
- Dieser Modus öffnet Verbindungen zum Passwort-Server und hält diese offen.
- Die Sicherheit des Samba-Servers bricht aufs Schlimmste zusammen, wenn der Passwort-Server mittendrin abgeschaltet werden sollte.
- In diesem Modus gibt es KEINEN Sicherheits-Account in der Domäne, um sicherzustellen, dass der Passwort-Server, der von Samba befragt wird, auch zur Domäne gehört.

Im Server-Sicherheitsmodus gibt der Samba-Server dem Client vor, im User-Level-Sicherheitsmodus zu agieren, und der Client schickt daraufhin ein Session Setup wie zuvor beschrieben. Der Samba-Server nimmt nun den Benutzernamen und das Passwort des Clients und schickt diese Daten exakt so, wie er sie bekommen hat, zum password server weiter. Wenn dieser Passwort-Server mit den Accountdaten einverstanden ist und in User Level-Sicherheit betrieben wird, akzeptiert der Samba-Server die Client-Verbindung. Dies erlaubt dem Samba-Server, einen anderen SMB-Server als password server zu nutzen.

Sie sollten wissen, dass am Anfang all dessen der Server dem Client auch mitteilt, ob eine Verschlüsselung der Daten stattfinden soll. Wenn dies auf dem Samba-Server konfiguriert ist, sendet der Server dem Client einen Krypto-Schlüssel, mit dem dann die Daten vom Client verschlüsselt werden. Samba unterstützt diese Verschlüsselung als Standard.

Der Parameter security = server bedeutet, dass der Samba-Server den Clients mitteilt, dass er im *user mode* betrieben wird, aber alle Passwort-Anfragen an einen anderen *user mode*-Server weiterleitet. Hierzu benötigt man einen weiteren Parameter, password server, der

auf den echten Authentifizierungsserver verweist. Dieser Passwort-Server kann ein anderer Samba-Server oder ein Windows-NT-Server sein.

ANMERKUNG

Falls Sie Samba im *Server-Sicherheitsmodus* betreiben, ist es äußerst wichtig, dass Sie den Parameter *password server* auf den genauen NetBIOS-Maschinen-Namen des Authentifizierungsservers setzen. Samba ist nicht in der Lage, dies über eine NetBIOS-Namens-Auflösung zu ermitteln, da die Auswahl des Authentifizierungsservers beliebig ist und nicht aus einem Domain-Namen ermittelt werden kann. Daraus folgt: Ein Samba-Server im *Server Security Mode* arbeitet so, wie man es als *workgroup mode* kennt.

4.3.5.1 Beispielkonfiguration

Benutzung von MS Windows NT als Authentifizierungsserver.

Diese Methode betrifft folgende Parameter in der `smb.conf`-Datei:

```
encrypt passwords = Yes
security = server
password server = NetBIOS_name_of_a_DC"
```

Es gibt zwei Verfahren, um ein Username/Passwort-Paar auf Gültigkeit zu überprüfen. Das eine nutzt die Informationen aus der Antwort, die als Teil der Authentifizierungsnachricht bereitgestellt wird, und das andere Verfahren wertet nur den Fehlercode aus.

Der Nachteil bei dieser Art der Konfiguration ist die Tatsache, dass Samba aus Sicherheitsgründen dem Passwort-Server einen erfundenen Benutzernamen und ein erfundenes Passwort sendet. Falls diese Accountdaten vom Passwort-Server abgelehnt werden, wechselt Samba zu einem alternativen Modus der Identifikation. Sollte das Netzwerk einen Benutzer nach einer gewissen Anzahl von fehlgeschlagenen Logins sperren, wird dies in dieser Konfiguration der Fall sein können. Sollte eine Website die Passwort-Eingabe nach einer gewissen Anzahl von fehlgeschlagenen Logins sperren, werden bei dieser Art der Konfiguration die Benutzer ausgesperrt.

Diese Art der Authentifizierung benötigt einen Standard-UNIX-Account für den User, der allerdings für andere System-Logins blockiert werden darf.

4.4 Passwort-Prüfung

MS Windows-Clients können verschlüsselte Passwörter (bekannt als NTLMv1 und MTLMv2) zur Anmeldung nutzen oder aber auch Klartext-Passwörter für eine einfache passwort-basierende Authentifizierung nutzen. Man sollte sich deutlich machen, dass das

SMB-Protokoll nicht vorsieht, dass sowohl Klartext- als auch verschlüsselte Passwörter innerhalb einer Authentifizierungsanfrage über ein Netzwerk verschickt werden.

Wenn verschlüsselte Passwörter verwendet werden, gibt es zwei verschiedene Arten, diese zu verschlüsseln:

- Ein MD5-Hash des Passworts (Unicode), besser bekannt als NT-Hash.
- Das Passwort wird in Großbuchstaben konvertiert und auf eine Länge von insgesamt 14 Byte gekürzt oder verlängert. Anschließend wird dieser String mit 5 Byte des NULL-Zeichens am Ende erweitert und geteilt, um zwei 56-Bit-DES-Schlüssel zu bilden, die zur Verschlüsselung eines „*magischen*“ 8-Byte-Wertes verwendet werden. Das Resultat hieraus ist der 16-Byte-LanMan-Hash.

MS Windows 95 vor SP 1 und MS Windows NT in den Versionen 3.x und 4.0 vor SP3 unterstützen beide Arten der Passwort-Authentifizierung. Alle Versionen von MS Windows nach den oben genannten Versionen unterstützen standardmäßig die Verwendung von Klartext-Passwörtern nicht mehr.

MS Windows-Clients haben die Eigenart, Netzwerk-Mappings zu verlieren, wenn diese länger als 10 Minuten nicht mehr verwendet wurden. Wenn der User ein Mapping nach dieser Zeit verwenden will, baut der Client die Verbindung erneut auf und verwendet dabei eine zwischengespeicherte Kopie des Passworts.

Als Microsoft den Standard-Passwort-Modus änderte, wurde die Unterstützung für das Cachen des Klartext-Passworts entfernt. Wenn man bei Windows durch Ändern der Registry-Einträge die Verwendung von Klartext-Passwörtern wieder einschalten würde, entfällt allerdings der oben beschriebene Support zum Zwischenspeichern der Passwörter. Dies hat zur Folge, dass es nicht gelingen wird, eine Verbindung von allein wiederherzustellen, wenn ein Client sie nach dem o.g. Timeout verworfen hat. Es ist also definitiv keine gute Idee, bei diesen Clients Klartext-Passwörter zu verwenden.

Folgende Parameter können als Workaround für Windows 9x/Me-Clients verwendet werden, die die Benutzernamen und Passwörter in Großbuchstaben umwandeln, bevor sie zum SMB-Server verschickt werden (Nur bei Verwendung von Klartext-Passwörtern).

```
password level = integer
username level = integer
```

Samba wird standardmäßig den Benutzernamen in Kleinbuchstaben umwandeln, bevor versucht wird, diesen in der lokalen Benutzerdatenbank zu authentifizieren. Da UNIX-Benutzernamen üblicherweise nur Kleinbuchstaben enthalten, wird der username level-Parameter nur selten verwendet.

UNIX-Systeme machen oftmals Gebrauch von gemischter Groß-/Kleinschreibung im Passwort. Dies hat zur Folge, dass bei Benutzung von Klartext-Passwörtern auf Windows 9x/Me-Systemen der Parameter password level auf die Anzahl an Großbuchstaben gesetzt werden muss, die in einem Passwort maximal vorkommen *können*. Beachten Sie bitte Folgendes: Bei Verwendung der traditionellen DES-Verschlüsselung der crypt()-Funktion hat eine Konfiguration password level von 8 case-insensitive Passwörter zur Folge, wie sie von Windows-Benutzern gesehen werden. Dies kann lange Login-Zeiten nach sich ziehen, bis ein Passwort angenommen wird bzw. alle Kombinationen fehlgeschlagen sind.

Die beste Lösung ist es, die Unterstützung von verschlüsselten Passwörtern zu aktivieren, wo immer Samba genutzt wird. Die meisten Versuche, die Registrierung von Windows dahingehend zu verändern, dass Klartext-Passwörter verwndet werden können, führen zu Beschwerden und Verärgerung der Anwender.

4.5 Häufige Fehler

Wir alle machen Fehler. Es ist okay Fehler zu machen, solange man sie an den richtigen Stellen zum richtigen Zeitpunkt macht. Ein Fehler, der zu einem Produktivitätsausfall führt, wird selten toleriert, wohingegen ein Fehler in einem Entwicklungslabor erwartet wird.

An dieser Stelle werfen wir einen Blick auf häufige Fehler, die Thema in Diskussionen der Samba-Mailing-Liste sind. Viele dieser Fehler sind vermeidbar, wenn Sie Ihre Hausaufgaben vor der Einführung von Samba machen. Einige sind das Ergebnis von Missverständnissen in Bezug auf die englische Sprache. Die englische Sprache hat viele Phrasen, die potenziell vage sind und die jemanden, dessen Muttersprache nicht Englisch ist, sehr verwirren können.

4.5.1 Was macht Samba zu einem Server?

Es wird oftmals angenommen, dass security = server bedeutet, dass Samba als Server agiert. Dies ist nicht so! Diese Einstellung bedeutet, dass Samba *versucht*, einen anderen SMB-Server für sich selbst als Quelle zur Authentifizierung zu verwenden.

4.5.2 Was macht Samba zu einem Domänencontroller?

Der `smb.conf`-Parameter security = domain macht Samba nicht zu einem Domänencontroller, sondern besagt, dass der Samba-Server einer Domäne als Mitglied angehören soll.

4.5.3 Was macht Samba zu einem Domänen-Mitglied?

Raten Sie! So machen es viele andere. Aber was auch immer Sie tun, glauben Sie nicht, dass security = user Samba zu einem Domänen-Mitglied werden lässt. Lesen Sie hier weiter: Kapitel 7 „Domänen-Mitgliedschaft“

4.5.4 Verlieren der Verbindung zum Passwort-Server

„*Warum gibt server_validate() einfach auf, statt die Verbindung zum Passwort-Server wieder aufzubauen? Da ich das SMB-Protokoll nicht so gut kenne, vermute ich, dass der Cluster-Server den Session-Key vom Passwort-Server zu den Client-Workstations weiterreicht, was bedeutet, dass die Passwort-Hashes der Clients nicht in einer folgenden Sitzung funktionieren, deren Session-Key anders wäre, somit muss server_validate() an dieser Stelle abbrechen.*“

Genau! Das ist der Grund, warum security = server ein gemeiner Hack ist. Bitte verwenden Sie security = domain; der security = server-Modus ist auch als Pass-through-Authentifizierung bekannt.

Kapitel 5

DIE KONTROLLE ÜBER EINE DOMÄNE

Viele nähern sich der Thematik der MS-Windows-Netzwerke mit falschen Vorstellungen. Das ist nicht schlimm, weil es uns anderen viele Möglichkeiten gibt, Hilfe zu bieten. Diejenigen, die wirklich helfen wollen, sind gut beraten, sich mit den bereits vorhandenen Informationen und der Dokumentation vertraut zu machen.

Wir möchten Ihnen empfehlen, diesen Abschnitt der Samba-Dokumentation gar nicht erst anzugehen, solange Sie nicht einige Grundlagen beherrschen. MS-Windows-Netzwerke sind gegenüber Fehlkonfigurationen nicht gerade tolerant. Anwender von MS-Windows-Netzwerken beschweren sich oft über dauernde Unannehmlichkeiten infolge „*kaputter*“ Netzwerk-Konfigurationen. Für viele jedoch beginnt die Arbeit mit MS-Windows-Netzwerken mit einem Domänencontroller, von dem erwartet wird, dass er auf irgendeine magische Art alle Netzwerk-Probleme lösen kann.

Das Diagramm in Abbildung 5.1 zeigt eine klassische Umgebung unter Verwendung einer MS-Windows-Sicherheitsdomäne (MS Windows Domain Security network environment). Die Workstations A, B und C repräsentieren eine Vielzahl physischer MS-Windows-Netzwerk-Clients.

Figure 5.1. Eine Beispiel-Domäne.

In der Samba-Mailing-liste kann man leicht viele weit verbreitete Netzwerk-Themen erkennen. Wenn Sie mit den folgenden Themen nicht vertraut sind, wird es helfen, die entsprechenden Abschnitte dieses HOWTOs zu lesen. Dies sind die häufigsten Ursachen für Probleme mit MS-Windows-Netzwerken:

- Grundlegende TCP/IP-Konfiguration
- NetBIOS Namensauflösung
- Authentifizierungskonfiguration
- Benutzer- und Gruppenkonfiguration
- Grundlegende Datei- und Verzeichnisrechte in UNIX/Linux
- Zusammenarbeit von MS-Windows-Clients in einer Netzwerkumgebung

Lassen Sie sich nicht abschrecken; an der Oberfläche erscheint ein MS-Windows-Netzwerk so simpel, dass es jeder einrichten kann. Tatsächlich ist es aber keine gute Idee, ein MS-Windows-Netzwerk ohne entsprechende Übung und Vorbereitung aufzusetzen. Aber lassen Sie uns unser erstes unauslöschliches Prinzip aus dem Weg räumen: *Es ist in Ordnung, Fehler zu machen!* Am richtigen Ort, zur richtigen Zeit sind Fehler die Essenz des Lernens. Es ist jedoch ganz und gar nicht in Ordnung, Fehler zu machen, die Produktivitätseinbußen verursachen und einer Organisation einen vermeidbaren finanziellen Verlust zufügen.

Wo ist der rechte Ort für Fehler? Nur dort, wo kein Schaden entstehen kann. Wenn Sie Fehler machen wollen, dann machen Sie diese bitte in einer Test-Umgebung, abseits von anderen Benutzern, auf eine Art, die anderen keine Probleme bereitet. Lernen Sie in einem Test-Netzwerk.

5.1 Eigenschaften und Vorzüge

Was ist der Hauptnutzen der Microsoft-Domänen-Sicherheit?

In einem Wort: *Single Sign On* oder, noch kürzer, SSO. Für viele ist dies der "Heilige Gral"des Windows-NT-Netzwerks und darüber hinaus. SSO erlaubt Benutzern eines gut konzipierten Netzwerks, sich auf jeder Workstation anzumelden, die Mitglied jener Domäne ist, zu der ihr Benutzer-Konto gehört (bzw. auf einer Workstation, die Mitglied einer Domäne ist, die ein geeignetes Vertrauensverhältnis zur eigenen Domäne hat). Dadurch können sie sich am Netzwerk anmelden und auf dessen Ressourcen zugreifen (Freigaben, Dateien und Drucker), als ob sie an ihrem Stamm-Rechner sitzen würden. Dies ist ein Merkmal des Domänen-Sicherheitsprotokolls.

Die Vorzüge von Domänen-Sicherheit eröffnen sich jenen, die einen Samba-PDC verwenden. Eine Domäne stellt einen eindeutigen Identifizierungsschlüssel für die Netzwerk-Sicherheit (network security identifier), kurz SID, zur Verfügung. Identifizierungs-Schlüssel für die Domänen-Benutzer- und -Gruppen-Sicherheit umfassen den SID plus einem relativen Identifizierungsschlüssel (RID), der sich eindeutig auf das jeweilige Konto bezieht. Benutzer- und Gruppen-SIDs (Netzwerk-SID plus RID) können dazu verwendet werden, so genannte Zugriffskontroll-Listen, besser bekannt als ACLs (Access Control Lists) zu erstellen, die, bezogen auf einzelne Netzwerk-Ressourcen, eine organisationsweite Zugriffskontrolle ermöglichen. UNIX-Systeme erkennen nur lokale SIDs.

ANMERKUNG

Netzwerk-Clients einer MS-Windows-Sicherheitsdomänen-Umgebung müssen Domänen-Mitglieder sein, um Zugriff auf die erweiterten Funktionalitäten zu erlangen. Eine Domänen-Mitgliedschaft beinhaltet mehr, als den Arbeitsgruppen-Namen auf den Domänen-Namen zu setzen. Sie erfordert das Anlegen eines Domänen-Kontos für die Workstation (genannt Maschinen-Konto). Lesen Sie Kapitel 7 „Domänen-Mitgliedschaft“ für mehr Informationen dazu.

Die folgenden Funktionalitäten sind in der Release Samba 3 neu:

- Windows NT4-Vertrauensdomänen
- Das Hinzufügen von Benutzern via „*User Manager for Domains*“. Dies kann von jedem MS-Windows-Client mit dem `Nexus.exe`-Toolkit für Windows 9x/Me oder mit dem SRVTOOLS.EXE-Paket für MS Windows NT4/200x/XP-Plattformen durchgeführt werden. Diese Pakete sind auf der Microsoft-Website verfügbar.
- Die Einführung mehrerer austauschbarer Benutzer-Konten-Backends (Authentifizierungs-Backends). Im Falle der Verwendung von LDAP als Backend profitiert Samba-3 von den Vorzügen eines Backends, das verteilt und repliziert werden kann sowie hochgradig skalierbar ist.
- Die Einführung voller Unicode-Unterstützung. Dies vereinfacht die Unterstützung internationaler Locales. Es ermöglicht außerdem die Verwendung von Protokollen, die Samba-2.2.x bereits unterstützte, jedoch mangels voller Unicode-Unterstützung nicht verwenden konnte.

Die folgenden Funktionalitäten werden von Samba-3 NICHT zur Verfügung gestellt:

- SAM-Replikation mit MS-Windows-NT4-Domänencontrollern (z.B. ein Samba-PDC und ein Windows NT-BDC oder vice versa). Dies bedeutet, dass Samba NICHT als BDC arbeiten kann, wenn der PDC Microsoft-basiert ist. Weiters bedeutet es, dass Samba Kontodaten NICHT auf MS-BDCs repliziert.
- Das Arbeiten als Windows 2000-Domänencontroller (z.B. Kerberos und Active Directory).
- Die Windows 200x/XP MMC-(Computer Management-)Konsole kann NICHT zum Betrieb eines Samba-3-Servers verwendet werden. Dazu können nur der MS Windows NT4 Domain Server Manager und der MS Windows NT4 Domain User Manager verwendet werden. Beide sind Bestandteil des später erwähnten SVRTOOLS.EXE-Pakets.

Windows 9x/Me/XP Home-Clients sind keine vollwertigen Domänen-Mitglieder - aus den hier erwähnten Gründen. Das Protokoll zur Unterstützung von Windows 9x/Me-Netzwerk(-Domänen)-Logons unterscheidet sich völlig von dem zur Unterstützung von NT4/Windows 200x-Netzwerk(-Domänen)-Logons und wurde einige Zeit offiziell unterstützt. Diese Clients

verwenden die alten LanMan-Netzwerk-Logon-Mechanismen, die in Samba ungefähr seit Serie Samba-1.9.15 unterstützt werden.

Samba-3 implementiert die Zuweisung von Gruppen zwischen Windows-NT-Gruppen und UNIX-Gruppen (dies ist wirklich sehr schwierig in kurzen Worten zu erklären). Dies wird umfassender in Kapitel **??** „Das Gruppen-Mapping zwischen MS Windows und UNIX“ behandelt.

Samba-3 muss (wie ein MS Windows NT4-PDC oder ein Windows 200x-AD) Benutzer- und Maschinen-Vertrauenskonten in einem passenden Daten-Backend ablegen (siehe Abschnitt 7.2). Mit Samba-3 können dazu mehrere Backends verwendet werden. Eine vollständige Erläuterung von Konten-Datenbank-Backends finden Sie in Kapitel **??** „Die Account-Datenbank“.

5.2 Grundlagen der Domänen-Verwaltung

Im Laufe der Jahre hat die allgemeine Auffassung von Domänen-Verwaltung eine fast schon mystische Gestalt angenommen. Bevor wir zu einem kurzen Überblick über Domänen-Verwaltung verzweigen, beschreiben wir die drei grundsätzlichen Typen von Domänencontrollern.

5.2.1 Typen von Domänencontrollern

- Primäre Domänencontroller
- Backup-Domänencontroller
- ADS-Domänencontroller

Der *primäre Domänencontroller* oder PDC spielt eine wichtige Rolle in MS Windows NT4. In der Windows 200x-Domänenverwaltungsarchitektur wird diese Rolle von Domänencontrollern übernommen. Die „*Folklore*“ schreibt vor, dass dies wegen seiner Rolle im MS Windows-Netzwerk der stärkste und schnellste Rechner im Netz sein sollte. So seltsam das an dieser Stelle klingen mag, der Wunsch nach guter allgemeiner Netzwerk-Performance erfordert zwingend, dass die gesamte Infrastruktur ausgewogen gestaltet wird. Es ist ratsam, mehr in Stand-alone-(Domänen-Mitglieds-)Server zu investieren als in die DCs.

Im Falle von MS Windows NT4-Domänen ist es der PDC, der eine neue Datenbank zur Domänen-Verwaltungs initiiert. Diese bildet einen Teil der Windows-Registrierung namens Security Account Manager (SAM). Sie spielt eine Schlüsselrolle bei der NT4-artigen Domänen-Benutzer-Authentifizierung und in der Synchronisation der Domänen-Authentifizierungsdatenbank mit Backup-Domänencontrollern.

In MS Windows 200x-Server-basierten Active-Directory-Domänen initiiert ein Domänencontroller eine mögliche Hierarchie von Domänencontrollern, von denen jeder seinen eigenen delegierten Verwaltungsbereich erhält. Der Master-Domänencontroller hat die Möglichkeit, jeden „*downstream controller*“ zu übergehen, jedoch hat ein „*downline controller*“ nur die Kontrolle über seine „*downline*“. Mit Samba-3 kann diese Funktionalität durch Verwendung eines Konten-Backends auf LDAP-Basis implementiert werden.

Neu in Samba-3 ist die mögliche Verwendung einer Backend-Datenbank, die dieselben Daten enthält wie eine NT4-artige SAM-Datenbank (eines der Registrierungs-Files)[1].

Der *Backup-Domänencontroller* oder BDC spielt eine Schlüsselrolle bei der Beantwortung von Netzwerk-Authentifizierungsanfragen. Der BDC ist darauf ausgerichtet, Logon-Anfragen vor dem PDC zu beantworten. In einem Netzwerk-Segment, das sowohl einen BDC als auch einen PDC beinhaltet, wird der BDC meist die Netzwerk-Logon-Anfragen bedienen. Der PDC wird diese dann beantworten, wenn der BDC überlastet ist. Ein BDC kann zum PDC ernannt werden. Wenn der PDC online ist, wenn der BDC zum PDC ernannt wird, wird der vorige PDC automatisch zum BDC zurückgestuft. Mit Samba-3 ist dieser Vorgang nicht automatisch; der PDC und der BDC müssen von Hand konfiguriert werden.

Bei der Installation von NT 4 wird die Entscheidung darüber getroffen, welcher Art von Maschine der Server angehören soll. Es ist möglich, einen BDC zu einem PDC zu ernennen und umgekehrt. Die einzige Möglichkeit, einen DC in einen Domänen-Mitgliedsserver oder einen Stand-alone-Server umzuwandeln, ist, ihn neu zu installieren. Die Wahlmöglichkeiten bei der Installation sind:

- *Primärer Domänencontroller / PDC* — der Server, der die Domänen-SAM begründet.
- *Backup Domänencontroller / BDC* — ein Server, der eine Kopie der Domänen-SAM anlegt.
- *Domänen-Mitgliedsserver* — ein Server, der keine Kopie der Domänen-SAM hält, jedoch seine Authentifizierungsinformationen von einem Domänencontroller bezieht.
- *Stand-alone-Server* — ein Server, der keine Rolle in der Synchronisation der Domänen-SAM spielt, seine eigene Authentifizierungsdatenbank führt und auch keine Rolle in der Domänen-Sicherheit übernimmt.

Bei der Verwendung von MS Windows 2000 wird die Konfiguration der Domänen-Verwaltung nach der Installation des Servers vorgenommen. Samba-3 kann als vollwertiges Mitglied einer Windows-200x-Server-Active-Directory-Domäne arbeiten.

Neu in Samba-3 ist die Fähigkeit, als vollwertiger MS-Windows-NT4-Domänencontroller zu arbeiten, mit Ausnahme der SAM-Replikationskomponenten. Bitte beachten Sie, dass Samba-3 auch die MS Windows 200x-Domänen-Verwaltungsprotokolle unterstützt.

Zum jetzigen Zeitpunkt ist jegliches Anzeichen dafür, dass Samba-3 als *Domänencontroller* im nativen ADS-Modus arbeiten kann, begrenzt und völlig experimenteller Natur. Diese Funktionalität sollte nicht verwendet werden, bis das Samba-Team formal die Unterstützung dafür anbietet. Sobald dies erfolgt, wird die Dokumentation revidiert werden, um alle Konfigurations- und Verwaltungsanforderungen vollständig widerzuspiegeln. Samba kann als NT4-DC in einer Windows 2000/XP-Umgebung arbeiten. Jedoch gibt es einige Kompromisse:

- Es gibt keine Maschinen-Policy-Dateien.
- Es gibt keine Gruppen-Policy-Objekte.
- Es gibt keine synchron ausgeführten AD-Logon-Skripts.

[1] Siehe auch Kapitel **??** „Die Account-Datenbank“.

- Die Active Directory-Management-Tools können nicht zur Benutzer- und Maschinen-Verwaltung verwendet werden.
- Änderungen an der Registrierung prägen die Hauptregistrierung, während mit AD keine bleibenden Veränderungen hinterlassen werden.
- Ohne AD kann die Funktion, spezifische Applikationen für spezifische Benutzer/Gruppen zu exportieren, NICHT genutzt werden.

5.2.2 Vorbereitungen für die Domänen-Verwaltung

Es gibt zwei Arten, wie MS Windows-Maschinen miteinander, mit anderen Servern und DCs zusammenarbeiten können: entweder als *Stand-alone*-Systeme, üblicherweise als *Workgroup*-Mitglieder bezeichnet, oder als vollwertige Teilnehmer eines Sicherheitssystems, die in der Regel als *Domain*-Mitglieder bezeichnet werden.

Beachten Sie, dass eine *Workgroup*-Mitgliedschaft keine spezielle Konfiguration erfordert, außer dass die Maschine so konfiguriert werden muss, dass die Netzwerk-Konfiguration einen gebräuchlichen Namen für den Workgroup-Eintrag enthält. Oft wird hierfür der Name WORKGROUP verwendet. Bei dieser Art der Konfiguration gibt es keine Maschinen-Vertrauenskonten und jegliches Konzept von Mitgliedschaft ist darauf beschränkt, dass alle in der Netzwerkumgebung auftauchenden Maschinen als logische Gruppe erscheinen. Zur Wiederholung und Klärung: *Der Workgroup-Modus beinhaltet keine Maschinen-Sicherheitskonten.*

Rechner, die Domänen-Mitglied sind, haben ein Maschinen-Konto in der Domänen-Konten-Datenbank. Eine spezielle Prozedur muss auf jeder Maschine ausgeführt werden, um eine Domänen-Mitgliedschaft zu erwerben. Diese Prozedur, die nur vom lokalen Administrator-Konto aus erfolgen kann, legt das Domänen-Maschinen-Konto an (falls es noch nicht existiert), und initialisiert dieses Konto. Wenn der Client sich erstmals in der Domäne anmeldet, wird ein Maschinen-Passwort-Wechsel ausgelöst.

> Anmerkung
>
>
>
> Wird Samba als Domänencontroller konfiguriert, müssen alle MS Windows NT4/200x/XP Professional-Clients als Domänen-Mitglieder konfiguriert werden, um den sicheren Betrieb des Netzwerks zu gewährleisten. Wenn eine Maschine nicht zum Domänen-Mitglied gemacht wird, wird sie sich wie eine Arbeitsgruppen(Stand-alone)-Maschine verhalten. Lesen Sie Kapitel 7 „Domänen-Mitgliedschaft“ für Informationen zur Domänen-Mitgliedschaft.

Folgendes ist nötig, um Samba-3 als einen MS Windows NT4-artigen PDC für MS-Windows-NT4/200x/XP-Clients zu konfigurieren:

- Konfiguration der Basisdienste TCP/IP und MS Windows Netzwerk

- Korrekte Zuweisung der Server-Rolle (security = user)
- Konsistente Konfiguration der Namensauflösung [2]
- Domänen-Logins für Windows NT4/200x/XP Professional-Clients
- Konfiguration von Roaming Profiles oder explizite Konfiguration, um die Verwendung lokaler Profile zu erzwingen
- Konfiguration von Netzwerk/System-Policies
- Hinzufügen und Verwalten von Domänen-Benutzer-Konten
- Konfiguration von MS Windows-Clients als Domänen-Mitglieder

Die folgenden Voraussetzungen sind erforderlich, um MS Windows 9x/Me-Clients bedienen zu können:

- Konfiguration der Basisdienste TCP/IP und MS Windows Netzwerk
- Korrekte Zuweisung der Server-Rolle (security = user)
- Netzwerk-Login-Konfiguration (da Windows 9x/Me/XP Home technisch gesehen keine Domänen-Mitglieder sind, haben sie auch nicht wirklich als solche an den Sicherheitsaspekten von Domänen Anteil) .
- Konfiguration von Roaming Profiles
- Konfiguration der Verwaltung der System Policy
- Installation des Netzwerk-Treibers „*Client for MS Windows Networks*“ und dessen Konfiguration, um sich in der Domäne anzumelden
- Setzen der Windows 9x/Me-Clients auf User Level Security, wenn es erwünscht ist, jeglichen Client-Zugriff auf Freigaben entsprechend der Domänen-Benutzer/Gruppen zu verwalten
- Hinzufügen und Verwalten von Domänen-Benutzer-Konten

ANMERKUNG

Roaming Profiles und System/Network Policies sind fortgeschrittene Themen der Netzwerk-Verwaltung, die in den Kapiteln Kapitel **??** „Das Management von Desktop-Profilen“ und Kapitel **??** „System und Zugriffsrichtlinien“ behandelt werden. Jedoch sind diese Themen für einen Samba-PDC nicht so entscheidend, da sie eng mit den Windows NT-Netzwerk-Konzepten zusammenhängen.

Ein Domänencontroller ist ein SMB/CIFS-Server, der:

[2] Siehe Kapitel 10 „Netzwerk-Browsing“, und Kapitel **??** „Samba in MS-Windows-Netzwerke integrieren“.

- sich selbst als Domänencontroller registriert und anbietet (sowohl durch NetBIOS-Broadcasts als auch durch verschiedene Namensregistrierungen, entweder durch Mailslot-Broadcasts über UDP-Broadcasts, einen WINS-Server über UDP-Unicast oder über DNS und Active Directory).
- den NETLOGON-Dienst anbietet. (Dies ist tatsächlich eine Sammlung von Diensten, die über mehrere Protokolle laufen. Zu ihnen zählen der LanMan-Logon-Dienst, der Netlogon-Dienst, der Local-Security-Account-Dienst und Abwandlungen dieser Dienste.)
- eine Freigabe namens NETLOGON anbietet.

Es ist ziemlich einfach, Samba so zu konfigurieren, dass er all dies zur Verfügung stellt. Jeder Samba-Domänencontroller muss den NETLOGON-Dienst anbieten, der von Samba als domain logons-Funktionalität bezeichnet wird (nach dem Parameter in der `smb.conf`-Datei). Außerdem muss ein Server in einer Samba-3-Domäne sich selbst als Domain Master Browser bekannt geben [3]. Dies veranlasst den PDC dazu, einen domänen-spezifischen NetBIOS-Namen zu beanspruchen, der ihn als Domain Master Browser für die gegebene Domäne/Workgroup identifiziert. Lokale Master Browser in derselben Domäne/Workgroup und in broadcast-isolierten Subnetzen erfragen dann eine komplette Kopie der „*browse list*“ für das gesamte WAN. Browser-Clients kontaktieren daraufhin ihren lokalen Master Browser und erhalten die „*browse list*“ der gesamten Domäne statt nur der Liste für ihr broadcast-isoliertes Subnetz.

5.3 Domänen-Verwaltung — Beispielkonfiguration

Der erste Schritt, um einen funktionierenden Samba-PDC zu erstellen, besteht darin, die nötigen Parameter in `smb.conf` zu verstehen. Ein Beispiel einer `smb.conf` für einen PDC finden Sie in Beispiel 5.3.1.

Die grundlegenden Optionen, die in Beispiel 5.3.1 gezeigt werden, werden wie folgt erklärt:

passdb backend Dies enthält sämtliche Information zu Benutzer- und Gruppenkonten. Akzeptable Werte für einen PDC sind: *smbpasswd, tdbsam* und *ldapsam*. Der „*guest*“-Eintrag stellt Standard-Konten zur Verfügung und ist standardmäßig vorhanden, es besteht keine Notwendigkeit, ihn explizit hinzuzufügen. Wo der Einsatz von Backup-Domänen-Controllern (BDCs) beabsichtigt ist, ist die einzige logische Wahl die Verwendung von LDAP, so dass die passdb verteilt werden kann. Die tdbsam- und smbpasswd-Dateien können nicht effektiv verteilt werden und sollten daher nicht verwendet werden.

Parameter zur Domänen-Verwaltung Die Parameter *os level, preferred master, domain master, security, encrypt passwords* und *domain logons* spielen eine wichtige Rolle bei der Unterstützung von Domänen-Kontrolle und Netzwerk-Anmeldung.

Das *os level* muss auf einen Wert von mindestens 32 gesetzt werden. Ein Domänencontroller muss auch der Domänen-Master-Browser sein, er muss auf

[3] Siehe Kapitel 10 „Netzwerk-Browsing“.

Beispiel 5.3.1. smb.conf, um einen PDC einzurichten

```
[global]
        netbios name = BELERIAND
        workgroup = MITTELERDE
        passdb backend = tdbsam
        os level = 33
        preferred master = yes
        domain master = yes
        local master = yes
        security = user
        domain logons = yes
        logon path = \\%N\profiles\%u
        logon drive = H:
        logon home = \\homeserver\%u\winprofile
        logon script = logon.cmd

[netlogon]
        path = /var/lib/samba/netlogon
        read only = yes
        write list = ntadmin

[profiles]
        path = /var/lib/samba/profiles
        read only = no
        create mask = 0600
        directory mask = 0700
```

user mode security gesetzt sein, muss MS-kompatibel verschlüsselte Passwörter unterstützen und muss den Netzwerk-Anmelde-Dienst (Domänen-Anmeldungen) anbieten. Verschlüsselte Passwörter müssen aktiviert sein. Mehr Details dazu finden Sie in Kapitel **??** „Die Account-Datenbank“.

Umgebungsparameter Die Parameter *logon path, logon home, logon drive* und *logon script* sind Umgebungseinstellungen, die dabei helfen, Client-Anmeldungen zu ermöglichen, und die automatisierte Kontrollmechanismen zur Verfügung stellen, um Overheads im Netzwerk-Management zu verringern. Siehe die Manpage für Informationen zu diesen Parametern.

NETLOGON-Freigabe Die NETLOGON-Freigabe spielt eine zentrale Rolle bei der Unterstützung von Domänen-Anmeldungen und Domänen-Mitgliedschaft. Diese Freigabe wird von allen MS-Domänen-Controllern zur Verfügung gestellt. Sie wird dazu verwendet, um Anmelde-Skripts bereitzustellen, um NT Richtlinien-Dateien (wie NTConfig.POL) zu speichern, aber auch, um andere gängige Werkzeuge zur Verfügung zu stellen, die für den Anmeldevorgang gebraucht werden. Dies ist eine essenzielle

Freigabe auf einem Domänencontroller.

PROFILE-Freigabe Diese Freigabe wird zur Speicherung von Benutzer-Desktop-Profilen verwendet. Jeder Benutzer muss ein Verzeichnis im root-Verzeichnis dieser Freigabe haben. Dieses Verzeichnis muss für den Benutzer Schreibrechte haben und global lesbar sein. Samba-3 hat ein VFS-Modul namens „*fake_permissions*“, das auf dieser Freigabe installiert werden kann. Das erlaubt es einem Samba-Administrator, das Verzeichnis read-only für jeden zu setzen. Natürlich ist dies nur sinnvoll, nachdem das Profil richtig erstellt worden ist.

ANMERKUNG

Die obigen Parameter bilden einen vollständigen Satz von Parametern, der den Arbeitsmodus des Servers definiert. Die folgenden `smb.conf`-Parameter sind die unbedingt notwendigen:

```
netbios name = BELERIAND
workgroup = MITTELERDE
domain logons = Yes
domain master = Yes
security = User
```

Die zusätzlichen Parameter, die in der längeren Auflistung oben gezeigt werden, bedürfen einer weitergehenden Erklärung.

5.4 ADS-Domänen-Verwaltung mit Samba

Samba-3 ist kein Active Directory Server und kann sich auch nicht so verhalten. Samba-3 kann nicht wirklich wie ein primärer Domänencontroller von Active Directory funktionieren. Die Protokolle für einige Funktionalitäten von AD-DCs wurden teilweise auf experimenteller Basis implementiert. Bitte erwarten Sie nicht, dass Samba-3 diese Protokolle unterstützt. Verlassen Sie sich nicht auf irgendeine derartige Funktionalität, weder jetzt noch in der Zukunft. Das Samba-Team könnte diese experimentellen Features entfernen oder deren Verhalten verändern. Dies wird erwähnt, um jenen zu helfen, die "geheimeFähigkeiten von Samba-3 entdeckt haben und danach gefragt haben, wann diese Funktionalitäten vervollständigt sein werden. Die Antwort darauf ist: „*Vielleicht bald. Vielleicht nie!*“

Um sicher zu sein: Samba-3 wurde entworfen, um den größten Teil der Funktionalität zur Verfügung zu stellen, die MS Windows NT4-artige Domänencontroller anbieten. Samba-3 hat nicht alle Fähigkeiten von Windows NT4, aber es hat einige Eigenschaften, die Windows NT4-DCs nicht haben. Kurz gesagt, Samba-3 ist nicht NT4, Samba-3 ist nicht Windows Server 200x, Samba-3 ist kein AD-Server. Wir hoffen, dass dies kurz und einfach genug ist, um für alle verständlich zu sein.

5.5 Konfiguration der Domänen- und Netzwerk-Anmeldung

Das Thema der Domänen- oder Netzwerk-Anmeldung wird hier behandelt, weil es einen integralen Teil der essenziellen Funktionen eines Domänencontrollers darstellt.

5.5.1 Domänen-Netzwerks-Anmelde-Dienst

Alle Domänencontroller müssen den netlogon-Dienst ausführen (*domain logons* in Samba). Ein Domänencontroller muss mit domain master = Yes konfiguriert werden (der PDC); auf allen BDCs muss domain master = No gesetzt werden.

5.5.1.1 Beispiel für eine Konfiguration

Beispiel 5.5.1. smb.conf, um einen PDC einzurichten

```
[global]
        domain logons = Yes
        domain master = (Yes on PDC, No on BDCs)

[netlogon]
        comment = Network Logon Service
        path = /var/lib/samba/netlogon
        guest ok = Yes
        browseable = No
```

5.5.1.2 Der spezielle Fall von MS Windows XP Home Edition

Um es unmissverständlich auszudrücken: Es ist NICHT MÖGLICH, einen Rechner mit MS Windows XP Home Edition in Ihre MS Windows NT4- oder ADS-Domäne zu integrieren. Die einzige Möglichkeit ist der Erwerb eines Upgrades von MS Windows XP Home Edition auf MS Windows XP Professional.

ANMERKUNG

MS Windows XP Home Edition besitzt nicht die Fähigkeit, sich jeglicher Art von Domäne anzuschließen. Im Unterschied zu MS Windows 9x/Me fehlt MS Windows XP Home Edition auch völlig die Fähigkeit, sich an einem Netz anzumelden.

Wir haben es Ihnen gesagt, fragen Sie also bitte NICHT auf der Samba-Mailing-Liste oder mailen Sie auch NICHT an die Mitglieder des Samba-Teams, um zu erkunden, wie dies

machbar wäre. Es ist NICHT MÖGLICH. Wenn es möglich ist, dann würde es Ihr Software-Lizenz-Abkommen mit Microsoft verletzen, und wir empfehlen, dies NICHT zu tun.

5.5.1.3 Der spezielle Fall von Windows 9x/Me

Eine Domäne und eine Arbeitsgruppe sind in den Begriffen des Netzwerk-Suchdienstes exakt dasselbe. Der Unterschied ist, dass mit einer Domäne eine verteilbare Anmelde-Datenbank verknüpft ist, die für sichere Anmeldungen an einem Netzwerk dient. Außerdem können andere Zugriffsberechtigungen an Benutzer vergeben werden, wenn sie sich erfolgreich an einem Domänen-Logon-Server anmelden. Samba-3 tut dies nun in derselben Weise wie MS Windows NT/200x.

Der SMB-Client, der sich an einer Domäne anmeldet, erwartet, dass jeder beliebige Server in der Domäne dieselbe Anmelde-Information akzeptiert. Die Netzwerk-Such-Funktionalität von Domänen und Arbeitsgruppen ist identisch und wird in dieser Dokumentation in den Abschnitten zum Browsing erklärt. Wir möchten anmerken, dass sich das Browsing völlig orthogonal zur Unterstützung von Anmeldungen verhält.

In diesem Abschnitt behandeln wir Themen in Bezug auf das Single-Logon-Netzwerk-Modell. Samba unterstützt Domänen-Anmeldungen, Netzwerk-Anmelde-Skripts und Benutzerprofile für MS Windows for Workgroups- und MS Windows 9X/ME-Clients, die im Mittelpunkt dieses Abschnitts stehen.

Wenn ein SMB-Client sich in einer Domäne anmelden will, sendet er Anfragen nach einem Anmelde-Server aus. Der erste, der antwortet, bekommt den Job und überprüft das Passwort unter Verwendung jenes Mechanismus, den der Samba-Administrator installiert hat. Es ist möglich (wird aber nicht empfohlen), eine Domäne anzulegen, in der die Benutzerdatenbank nicht von den Servern geteilt wird, d.h., sie sind effektiv Arbeitsgruppen-Server, die sich als Teilnehmer an einer Domäne bewerben. Dies demonstriert, wie sehr sich die Authentifikation einerseits von Domänen unterscheidet, dass sie andererseits aber eng mit ihnen verknüpft ist.

Unter Verwendung dieser Eigenschaften können Sie Ihre Clients ihre Anmeldung via Samba-Server überprüfen lassen und sie dazu veranlassen, bei der Netzwerkanmeldung ein Skript auszuführen und ihre Einstellungen, Desktops und Startmenüs herunterzuladen.

MS Windows XP Home Edition ist nicht fähig, sich einer Domäne anzuschließen, und erlaubt keine Verwendung von Domänenanmeldungen.

Bevor wir mit den Konfigurationsanleitungen beginnen, lohnt es sich, sich anzusehen, wie ein Windows 9x/Me-Client eine Anmeldung durchführt:

1. Der Client versendet über einen Broadcast (an die IP-Broadcast-Adresse des Subnetzes, in dem er sich befindet) eine NetLogon-Anfrage. Diese wird an den NetBIOS-Namen DOMÄNE<#1c> auf dem NetBIOS-Layer gesandt. Der Client wählt die erste Antwort, die er erhält, die den NetBIOS-Namen des zu verwendenden Anmeldeservers im Format `\\SERVER` enthält.

2. Der Client verbindet sich mit diesem Server, meldet sich an (führt ein SMBsessetupX aus) und verbindet sich dann mit der IPC$-Freigabe (unter Verwendung eines SMBtconX).

3. Der Client führt eine Anfrage vom Typ NetWkstaUserLogon aus, die den Namen des Anmeldeskripts des Benutzers zurückgibt.
4. Der Client verbindet sich dann mit der Netlogon-Freigabe und sucht nach dem angegebenen Skript. Wenn es gefunden wird und gelesen werden kann, wird es geladen und vom Client ausgeführt. Danach trennt der Client die Verbindung mit der Netlogon-Freigabe.
5. Der Client sendet eine Anfrage vom Typ NetUserGetInfo an den Server, um die Home-Freigabe des Benutzers zu erhalten, die dazu benutzt wird, um nach Profilen zu suchen. Da die Antwort auf die NetUserGetInfo-Anfrage nicht viel mehr enthält als die Home-Freigabe des Benutzers, müssen Profile für Windows 9x-Clients im Home-Verzeichnis des Benutzers liegen.
6. Der Client verbindet sich mit der Home-Freigabe des Benutzers und sucht nach dem Benutzerprofil. Wie sich herausstellt, können Sie die Home-Freigabe als Freigabe und Pfad angeben, zum Beispiel als `\\server\fred\.winprofile`. Wenn die Profile gefunden werden, werden sie eingebunden.
7. Der Client trennt die Verbindung mit der Home-Freigabe des Benutzers und verbindet sich wieder mit der Netlogon-Freigabe und sucht nach `CONFIG.POL`, der Policies-Datei. Wenn diese gefunden wird, wird sie gelesen und eingebunden.

Der Hauptunterschied zwischen einem PDC und einem Windows 9x/Me-Anmelde-Server ist:

- Die Verschlüsselung von Passwörtern ist für einen Windows 9x/Me-Anmelde-Server nicht notwendig. Aber denken Sie daran, dass seit MS Windows 98 die Standardeinstellung besagt, dass die Unterstützung von Klartext-Passwörtern deaktiviert ist. Sie kann mit den in Kapitel **??** „System und Zugriffsrichtlinien“ beschriebenen Änderungen aktiviert werden.
- Windows 9x/Me-Clients benötigen und benutzen KEINE Maschinen-Vertrauenskonten.

Ein Samba-PDC wird sich wie ein Windows 9x/Me-Anmelde-Server verhalten; schließlich stellt er all die Anmelde-Dienste zur Verfügung, die MS Windows 9x/Me erwartet.

ANMERKUNG

Von der Verwendung von Klartext-Passwörtern wird dringend abgeraten. Wo immer sie verwendet werden, können sie ganz einfach mit Netzwerk-Sniffern abgehört werden.

5.5.2 Sicherheitsmodus und Master Browser

Wir müssen noch ein paar Anmerkungen machen, um einige offene Fragen zu klären. Es gab viele Diskussionen darüber, ob es richtig sei, Samba als Domänencontroller in anderen Sicherheitsmodi als „*user*“ zu konfigurieren. Der einzige Modus, der aus technischen

Gründen nicht funktionieren wird, ist der Modus der Freigaben-Sicherheit. Domänen- und Server-Modus-Sicherheit sind in Wirklichkeit einfach nur Abwandlungen der SMB-Benutzer-Ebenen-Sicherheit.

Tatsächlich hängt dieses Thema auch eng mit der Debatte zusammen, ob Samba der Domänen-Master-Browser für seine Domäne sein muss, wenn er als DC arbeitet. Auch wenn es technisch möglich sein mag, einen Server so zu konfigurieren (schließlich sind Browsing und Domänenanmeldungen zwei völlig verschiedene Funktionen), ist es doch keine gute Idee, dies zu tun. Sie sollten sich daran erinnern, dass der DC den DOMAIN<#1b> NetBIOS-Namen registrieren muss. Dies ist der Name, der von den Windows-Clients verwendet wird, um den DC ausfindig zu machen. Windows-Clients unterscheiden nicht zwischen dem DC und dem DMB. (Ein DMB ist ein Domänen-Master-Browser — siehe Abschnitt 10.4.1.) Aus diesem Grunde ist es ratsam, den Samba DC auch als DMB zu konfigurieren.

Kommen wir nun zu dem Thema zurück, wie man einen Samba-DC so konfiguriert, dass er einen Modus verwendet, der von security = user abweicht. Wenn ein Samba-Rechner so konfiguriert ist, dass er einen anderen SMB-Server oder -DC verwendet, um Benutzeranmeldungen zu prüfen, dann ist es ein Faktum, dass irgendeine andere Maschine in diesem Netz (der password server) mehr über den Benutzer weiß, als der Samba-Rechner. In ungefähr 99% der Fälle ist dieser Rechner ein DC. Um nun im Domänen-Sicherheitsmodus zu arbeiten, ist es notwendig, den workgroup-Parameter auf den Namen der Windows NT-Domäne zu setzen (die bereits einen DC hat). Wenn die Domäne noch keinen DC hat, haben Sie noch keine Domäne.

Das Konfigurieren von Samba als DC für eine Domäne, die (per Definition) bereits einen PDC hat, bedeutet, sich seine Probleme selbst heraufzubeschwören. Deshalb sollten Sie den Samba-DC immer als DMB für seine Domäne konfigurieren und security = user setzen. Dies ist der einzige offiziell unterstützte Arbeitsmodus.

5.6 Häufige Fehler

5.6.1 „$“ darf nicht im Maschinen-Namen vorkommen

Ein Maschinenkonto, üblicherweise in `/etc/passwd` gespeichert, hat die Form des Maschinennamens, dem ein „$“ folgt. FreeBSD (und andere BSD-Systeme) legen keinen Benutzer mit einem „$“ im Namen an.

Das Problem liegt nur im Programm, das zum Anlegen des Eintrags verwendet wird. Einmal angelegt, funktioniert es perfekt. Legen Sie einen Benutzer ohne das „$“ an. Benutzen Sie dann den Befehl **vipw**, um den Eintrag zu editieren bzw. das „$“ hinzuzufügen. Oder legen Sie den ganzen Eintrag mit **vipw** an, wenn Sie wollen; stellen Sie sicher, dass Sie eine einmalige Benutzer-ID (UID) verwenden.

Anmerkung

Das Maschinen-Konto muss exakt den gleichen Namen wie die Workstation haben.

Anmerkung

Das UNIX-Tool **vipw** ist ein übliches Werkzeug für das direkte Editieren der Datei `/etc/passwd`.

5.6.2 Der Anschluss an die Domäne scheitert an einem bereits existierenden Maschinen-Konto

„Ich bekomme "You already have a connection to the Domain....öder Cannot join domain, the credentials supplied conflict with an existing set...", wenn ich ein Maschinen-Vertrauenskonto anlegen will.“

Dies passiert, wenn Sie versuchen, ein Maschinen-Vertrauenskonto von der betreffenden Maschine aus anzulegen, und bereits eine bestehende Verbindung (wie z.B. ein verbundenes Netzlaufwerk) zu einer Freigabe (oder zu IPC$) auf dem Samba-PDC haben. Der folgende Befehl trennt alle bestehenden Netzlaufwerksverbindungen:

```
C:\> net use * /d
```

Wenn die Maschine bereits ein *„Mitglied einer Arbeitsgruppe“* ist, die denselben Namen hat wie die Domäne, der Sie sich anschließen wollen (schlechte Idee), werden Sie dieselbe Meldung erhalten. Ändern Sie den Namen der Arbeitsgruppe in etwas anderes, egal was, rebooten Sie, und versuchen Sie es erneut.

5.6.3 Das System kann Sie nicht anmelden (C000019B)

„Ich schloss mich erfolgreich der Domäne an, aber nach dem Upgrade auf eine neue Samba-Release bekomme ich die Meldung The system cannot log you on (C000019B), Please try again or consult your system administrator", wenn ich versuche, mich anzumelden.“

Dies geschieht, wenn der Domänen-SID, der in der secrets.tdb-Datenbank gespeichert ist, geändert wird. Die häufigste Ursache für eine Änderung ist die Änderung des Domänen-Namens und/oder des Server-Namens (NetBIOS-Namens). Die einzige Lösung ist es, den originalen Domänen-SID wiederherzustellen oder den Domänen-Client aus der Domäne zu entfernen und neu einzubinden. Der Domänen-SID kann mit dem net- oder rpcclient-Werkzeug zurückgesetzt werden.

Zum Zurücksetzen oder Ändern des Domänen-SID können Sie den net-Befehl wie folgt verwenden:

```
root# net getlocalsid 'OLDNAME'
root# net setlocalsid 'SID'
```

Maschinen-Vertrauenskonten von Workstations arbeiten nur mit dem Domänen-SID (Netzwerk-SID). Wenn dieser SID sich ändert, können sich Domänen-Mitglieder (Workstations) nicht in der Domäne anmelden. Der originale Domänen-SID kann aus der secrets.tdb-Datenbank wiederhergestellt werden. Die Alternative ist es, jede einzelne Workstation aufzusuchen und neu an die Domäne anzuschließen.

5.6.4 Das Maschinen-Vertrauenskonto ist nicht erreichbar

„*Wenn ich versuche, mich der Domäne anzuschließen, bekomme ich die Nachricht TThe machine account for this computer either does not exist or is not accessible". Was ist falsch?*"

Dieses Problem wird dadurch verursacht, dass der PDC kein passendes Maschinen-Vertrauenskonto bereitstellt. Wenn Sie die add machine script-Methode zum Anlegen von Konten verwenden, ist dies ein Zeichen dafür, dass diese Methode nicht funktioniert hat. Stellen Sie sicher, dass der Benutzer des Domänen-Administrators richtig arbeitet.

Außerdem: Wenn Sie Konten von Hand erstellen, dann wurden diese nicht korrekt erstellt. Stellen Sie sicher, dass Sie den Eintrag für das Maschinen-Vertrauenskonto in der Datei `smbpasswd` auf dem Samba-PDC korrekt erstellt haben. Wenn Sie den Eintrag mit einem Editor erstellt haben, anstatt das Programm smbpasswd zu verwenden, sollten Sie kontrollieren, dass der Name des Kontos dem NetBIOS-Namen der Maschine entspricht, gefolgt von einem „*$*" (z.B. computer_name$). Es muss je einen Eintrag in `/etc/passwd` und in der Datei `smbpasswd` geben.

Manche Benutzer haben auch berichtet, dass inkonsistente Subnetz-Masken zwischen dem Samba-Server und dem NT-Client dieses Problem verursachen können. Stellen Sie sicher, dass diese Masken für Client und Server übereinstimmen.

5.6.5 Konto deaktiviert

„*Wenn ich versuche, mich einer Domäne von einer NT4/W200x-Workstation aus anzuschlie?en, bekomme ich die Nachricht, dass mein Konto deaktiviert wird.*"

Aktivieren Sie die Benutzer-Konten mit `smbpasswd -e` *Benutzername*. Dies wird normalerweise beim Anlegen eines Kontos ausgeführt.

5.6.6 Domänencontroller nicht verfügbar

„*Ein paar Minuten, nachdem Samba gestartet worden ist, bekommen die Clients den Fehler "Domain Controller Unavailable"*

“.

Ein Domänencontroller muss seine Rolle im Netzwerk bekannt geben. Dies braucht üblicherweise eine Weile. Haben Sie bis zu 15 Minuten Geduld, versuchen Sie es dann nochmals.

5.6.7 Ich kann mich nicht an einer Domänen-Mitglieds-Workstation anmelden, nachdem ich mich einer Domäne angeschlossen habe

Nach dem erfolgreichen Beitritt zu einer Domäne scheitern Benutzeranmeldungen mit einer von zwei Meldungen: die eine besagt, dass der DC nicht gefunden werden könne, die andere behauptet, dass das Konto nicht in der Domäne existiere bzw. dass das Passwort falsch sei. Dies kann durch imkompatible Einstellungen zwischen dem Windows-Client und dem Samba-3-Server verursacht werden, und zwar durch die *schannel-* (secure channel) oder *smb signing*-Einstellungen. Prüfen Sie die Einstellungen *client schannel, server schannel, client signing, server signing* durch das Ausführen von:

```
testparm -v | more
```

und prüfen Sie die Werte dieser Parameter.

Benutzen Sie auch die Microsoft Management Console — Local Security Settings. Dieses Werkzeug ist in der Systemsteuerung verfügbar. Die Policy-Einstellungen finden Sie im Bereich Local Policies/Security Options”: Sie erkennen Sie am Präfix *Secure Channel: ..., and Digitally sign .....*

Es ist wichtig, dass diese Einstellungen genauso gesetzt sind wie die des Samba-3-Servers.

Kapitel 6

BACKUP-DOMÄNEN-VERWALTUNG

Bevor Sie diesen Abschnitt lesen, sollten Sie sich vergewissern, dass Sie mit der Konfiguration eines Samba Domänen-Controllers, wie in Kapitel 5 „Die Kontrolle über eine Domäne“ beschrieben, vertraut sind.

6.1 Eigenschaften und Vorzüge

Dies ist eines der am schwierigsten zusammenzufassenden Kapitel. Was immer wir auch hier sagen, jemand wird seine eigenen Schlüsse ziehen und/oder mit Erwartungen an das Samba-Team herantreten, die entweder noch nicht erfüllbar sind oder mit einem komplett anderen Ansatz bei weitem effektiver erfüllt werden können. Sollten Sie ein andauerndes Anliegen haben, das nicht in diesem Buch behandelt wird, senden Sie bitte eine E-Mail an John H. Terpstra <mailto:jht@samba.org> , in der Sie Ihre Anforderungen und/oder Fragen klar erläutern, und wir werden unser Bestes tun, um Ihnen eine Lösung anzubieten.

Samba-3 ist in der Lage, als Backup-Domänen-Controller (BDC) für einen Samba-Primary-Domänencontroller (PDC) zu arbeiten. Ein Samba-3-PDC kann mit einem LDAP-Konten-Backend arbeiten. Das LDAP-Backend kann entweder ein gängiger Master-LDAP-Server oder ein LDAP-Slave-Server sein. Die Benutzung eines Slave-Servers hat den Vorteil, dass sich in dem Fall, dass der Master nicht verfügbar ist, die Clients noch immer am Netzwerk anmelden können. Dadurch erhält Samba ein hohes Maß an Skalierbarkeit und ist somit eine effektive Lösung für große Organisationen. Wenn Sie einen LDAP-Slave-Server für einen PDC verwenden, werden Sie für die ständige Verfügbarkeit des Master-Servers sorgen müssen - denn wenn der Slave den Master in einem falschen Moment heruntergefahren vorfindet, werden Sie Probleme mit dem Betrieb und der Stabilität haben.

Während es möglich ist, einen Samba-3-BDC mit einem anderen Backend als LDAP zu betreiben, muss dieses Backend doch eine Form von 2-Weg-Übertragung von Veränderungen vom BDC zum Master erlauben. Nur LDAP kann dies zum gegenwärtigen Zeitpunkt.

Die Verwendung einer Nicht-LDAP-Backend-SAM-Datenbank ist teilweise problematisch, weil Domänen-Mitgliedsserver und -Workstations regelmäßig das Passwort ihres Maschinen-Vertrauenskontos ändern. Das neue Passwort wird dann nur lokal gespeichert. Das bedeutet,

dass beim Fehlen einer zentral gespeicherten Konten-Datenbank (wie sie mit einer LDAP-basierten Lösung zur Verfügung steht) und BDC-Betrieb von Samba-3 der BDC-Anteil des Konten-Passworts nicht in die SAM des PDCs gelangen kann. Wenn dann die SAM des PDCs auf die BDCs repliziert wird, führt dies zum Überschreiben der SAM, die das veränderte Passwort enthält, was das Domänen-Vertrauensverhältnis aufhebt.

Wenn man die Anzahl der Kommentare und Fragen bedenkt, die sich um die Konfiguration eines BDCs ranken, macht es Sinn, jede mögliche Option zu bedenken und deren Vor- und Nachteile abzuwägen. Tabelle 6.1 listet mögliche Konfigurationen für eine PDC/BDC-Infrastruktur auf.

Tabelle 6.1. Optionen zur Verteilung der Domänen-Konten-Datenbank

PDC-Backend	BDC-Backend	Anmerkungen/Diskussion
Master-LDAP-Server	Slave-LDAP-Server	Die optimale Lösung, die hohe Integrität gewährleistet. Die SAM wird auf einen üblichen LDAP-Master-Server repliziert.
Einzelner zentraler LDAP-Server	Einzelner zentraler LDAP-Server	Eine funktionierende Lösung ohne Failover-Fähigkeiten. Dies ist eine brauchbare Lösung, jedoch nicht optimal.
tdbsam	tdbsam + **net rpc vampire**	Funktioniert NICHT mit Samba-3.0.0; könnte in einer späteren Release implementiert werden. Der Nachteil dieser Lösung ist, dass ein externer Prozess die Integrität der Konten-DB überwacht. Diese Lösung erscheint für Sites interessant, die die Komplexität von LDAP vermeiden wollen. Der Befehl **net rpc vampire** wird verwendet, um die Domänen-Konten des PDCs mit dem BDC zu synchronisieren.
tdbsam	tdbsam + **rsync**	Verwenden Sie diese Konfiguration NICHT. Sie funktioniert nicht, weil die tdb-files geöffnet sind und deren Daten noch nicht auf die Platte geschrieben worden sein könnten. Verwenden Sie **rsync**, um die tdb-files vom PDC auf den BDC zu synchronisieren.
smbpasswd Datei	smbpasswd Datei	Verwenden Sie diese Konfiguration NICHT. Dies ist keine elegante Lösung wegen der Verzögerungen bei der Synchronisation. Verwenden Sie **rsync**, um die tdb-Dateien vom PDC auf den BDC zu synchronisieren. Kann zum Funktionieren gebracht werden, wenn Sie einen **cron**-Job zur Synchronisation verwenden.

6.2 Essenzielle Hintergrund-Informationen

Ein Domänen-Controller ist eine Maschine, die imstande ist, Anmeldeanforderungen von Netzwerk-Workstations zu beantworten. Microsoft LanManager und IBM LanServer waren

zwei frühe Produkte, die diese Fähigkeit zur Verfügung stellten. Diese Technologie wurde als das LanMan Netlogon-Service bekannt.

Als MS Windows NT3.10 veröffentlicht wurde, unterstützte es eine neue Art der Domänen-Verwaltung und damit eine neue Form von Netzwerk-Anmelde-Dienst, die einen erweiterte Funktionalität hat. Dieser Dienst wurde als NT-NetLogon-Service bekannt. Die Natur dieses Dienstes hat sich im Laufe der Evolution von MS Windows NT verändert, und der NT-NetLogon-Service bietet heute ein komplexes Feld von Diensten, die ein kompliziertes Spektrum von Technologien abdecken.

6.2.1 Domänen-Verwaltung im Stil von MS Windows NT4

Wenn sich ein Benutzer an einer Windows NT4/200x/XP Professional-Workstation anmeldet, verbindet sich die Workstation mit einem Domänencontroller (Authentifikationsserver), um zu prüfen, ob der Benutzername und das Passwort, die vom Benutzer eingegeben wurden, gültig sind. Wenn die eingegebenen Informationen nicht mit der Konto-Information übereinstimmen, die in der Domänen-Verwaltungsdatenbank (die SAM oder Security-Account-Manager-Datenbank) abgelegt ist, wird ein Satz von Fehler-Codes an die Workstation zurückgeschickt, die die Anmelde-Anfrage gestellt hat.

Wenn das Benutzername/Passwort-Paar überprüft worden ist, antwortet der Domänencontroller (Authentifikationsserver) mit einer vollständigen Aufzählung der Konto-Informationen, die zu diesem Benutzer in der Benutzer- und Maschinen-Konten-DB für diese Domäne gespeichert sind. Diese Informationen enthalten ein komplettes Netzwerk-Zugriffsprofil für den Benutzer, aber schließt jegliche Informationen aus, die für das Desktop-Profil des Benutzers spezifisch sind, oder schließt zu diesem Zweck alle Desktop-Profile für jene Gruppen aus, denen der Benutzer angehört. Die Informationen enthalten Passwort-Zeit-Limits, Überprüfungen auf die Einzigartigkeit des Passworts, Zeitlimits für den Netzwerkzugriff, Information über die Gültigkeit von Konten, Namen der Maschinen, von denen aus der Benutzer auf das Netzwerk zugreifen kann, und vieles mehr. All diese Informationen wurden von allen Versionen von MS Windows NT (3.10, 3.50, 3.51, 4.0) in der SAM gespeichert.

Die Konten-Informationen (Benutzer und Maschine) werden auf Domänencontrollern in zwei Dateien gespeichert; eine enthält die Sicherheitsinformationen, die andere die SAM. Diese werden in gleichnamigen Dateien im Verzeichnis `C:\Windows NT\System32\config` gespeichert. Dies sind die Dateien, die in die Replikation der SAM involviert sind, wenn Backup-Domänencontroller im Netzwerk vorhanden sind.

Es gibt zwei Situationen, in denen man Backup-Domänencontroller installieren sollte:

- Im lokalen Netzwerk des PDCs, wenn es viele Workstations gibt und/oder wenn der PDC generell sehr stark ausgelastet ist. In diesem Fall werden die BDCs Anmelde-Anforderungen übernehmen und mithelfen, die Robustheit des Netzes zu erhöhen.
- In jeder entfernten Filiale/Abteilung/Installation, um den WAN-Verkehr zu reduzieren und um die Stabilität der Netzwerk-Operationen zu erhöhen. Das Design des Netzwerks und das strategische Platzieren von BDCs zusammen mit einer Implementierung, die den Client-Netzwerk-Austausch möglichst lokal hält, wird den Bedarf an WAN-Bandbreite minimieren helfen (und damit auch deren Kosten senken).

Die Interaktion des PDC mit seinen BDCs in einem Windows NT4-Environment ist es wert, hier erwähnt zu werden. Der PDC enthält die Master-Kopie der SAM. Falls ein Administrator eine Änderung an der Benutzer-Konten-Datenbank vornimmt, während er physisch im LAN des PDCs ist, wird die Veränderung wahrscheinlich direkt am PDC durchgeführt, anstatt in der Master-Kopie der SAM. Sollte diese Veränderung in einer Zweigstelle durchgeführt werden, wird die Änderung wahrscheinlich in einem Delta-File auf dem lokalen BDC gespeichert. Der BDC wird dann einen Trigger an den PDC senden, um die Synchronisation der SAM zu beginnen. Dann wird der PDC das Delta-File vom BDC anfordern und es auf die Master-SAM anwenden. Danach wird der PDC alle BDCs in der Domäne kontaktieren und sie per Trigger veranlassen, sich das Update zu holen und es in ihre eigene Kopie der SAM einzuspielen.

Samba-3 kann nicht an wirklicher SAM-Replikation teilnehmen und ist daher nicht geeignet, exakt dieselben Protokolle zu verwenden wie MS Windows NT4. Ein Samba-3-BDC wird keine SAM-Update-Delta-Files generieren. Der Samba-3-BDC wird nicht mit einem PDC (NT4 oder Samba) zusammenarbeiten, um die SAM mittels Delta-Files von BDCS zu synchronisieren.

Samba-3 kann nicht als BDC für einen MS Windows NT4-PDC arbeiten, und Samba-3 kann nicht korrekt als PDC für einen MS Windows NT4-BDC arbeiten. Sowohl Samba-3 als auch MS Windows NT4 können als BDC für ihren eigenen Typ von PDC arbeiten.

Der BDC speichert eine *Read-only*-Version der SAM, mit deren Hilfe er Netzwerk-Anmelde-Anfragen bearbeiten und User authentifizieren kann. Der BDC kann damit fortfahren, diesen Dienst anzubieten, insbesondere dann, wenn die WAN-Verbindung zum PDC unterbrochen ist. Ein BDC spielt eine sehr wichtige Rolle, sowohl bei der Aufrechterhaltung der Domänen-Sicherheit als auch für die Integrität des Netzwerks.

Falls der NT4-PDC außer Betrieb genommen werden muss oder falls er ausfällt, kann einer der NT4-BDCs zu einem PDC „*befördert*“ werden. Wenn dies geschieht, während der originale NT4-PDC online ist, wird dieser automatisch zu einem NT4-BDC „*degradiert*“. Dies ist ein wichtiger Aspekt des Managements von Domänencontrollern. Es sollte bemerkt werden, dass Samba-3-BDCs NICHT auf diese Art zu PDCs befördert werden können, da die nötige Rekonfiguration von Samba Änderungen an `smb.conf` bedingt.

6.2.1.1 Beispiel einer PDC-Konfiguration

Seit der Version 2.2 unterstützt Samba offiziell Domänen-Anmeldungen für alle aktuellen Windows-Clients, einschließlich Windows NT4, 2003 und XP Professional. Um Samba als PDC zu betreiben, müssen einige Parameter im *[global]*-Abschnitt von `smb.conf` gesetzt werden. Sehen Sie sich Beispiel 6.2.1 an. Dies ist ein Beispiel für die auf jeden Fall erforderlichen Einstellungen.

Einige andere Dinge wie eine *[homes]*- und eine *[netlogon]*-Freigabe müssen ebenfalls in Verbindung mit Einstellungen für den Profil-Pfad, das Home-Verzeichnis des Benutzers usw. gesetzt werden. Dies wird in diesem Kapitel nicht behandelt; mehr Informationen dazu finden Sie in Kapitel 5 „Die Kontrolle über eine Domäne“.

Beispiel 6.2.1. Minimale smb.conf für einen PDC in Verbindung mit einem BDC-LDAP-Server auf dem PDC

```
workgroup = MITTELERDE
passdb backend = ldapsam://localhost:389
domain master = yes
domain logons = yes
```

6.2.2 Bemerkungen zur LDAP-Konfiguration

Wenn man einen Master- und einen Slave-LDAP-Server konfiguriert, ist es ratsam, den Master-LDAP-Server als PDC und die Slave-LDAP-Server als BDCs zu verwenden. Es ist nicht unbedingt notwendig, Slave-LDAP-Server zu verwenden, auch wenn es viele Administratoren tun werden wollen, um die Redundanz zu erhöhen. Natürlich können ein oder mehrere BDCs jeglichen Slave-LDAP-Server nutzen. Auch dann ist es wieder möglich, einen einzelnen LDAP-Server für das ganze Netzwerk zu verwenden.

Wenn man einen Master-LDAP-Server konfiguriert, der Slave-LDAP-Server haben wird, darf man nicht vergessen, dies in der Datei `/etc/openldap/slapd.conf` zu konfigurieren. Denken Sie daran, dass der DN eines Server-Zertifikats das CN-Attribut zur Benennung des Servers verwenden muss und dass CN den vollen Domain-Namen (FQDN = fully qualified domain name) des Servers beinhalten muss. Weitere Aliases und Wildcards können in der subjectAltName-Zertifikatserweiterung abgelegt werden. Die Kommunikation zwischen LDAP-PDC und LDAP-BDC muss komplett verschlüsselt ablaufen. Dazu können Sie Zertifikate verwenden. Mehr Details zu Server-Zertifikaten finden Sie in der RFC2830.

Installieren Sie keinen Samba-PDC auf einem OpenLDAP-Slave-Server. Das Hinzufügen von Client-Maschinen zur Domäne wird in dieser Konfiguration fehlschlagen, da die Veränderung am Maschinen-Konto im LDAP-Baum auf dem Master-LDAP-Server stattfinden muss. Dies wird nicht schnell genug auf den Slave-Server repliziert, den der PDC abfragt. Daher gibt es auf der Client-Maschine eine Fehlermeldung, die besagt, dass es nicht möglich sei, die Konto-Informationen richtig zu setzen. Das Maschinen-Konto wird auf dem LDAP-Server angelegt, aber die Passwort-Felder werden leer bleiben. (Anmerkung: Zur Lösung dieser Problematik wurde mit Samba 3.0.1 der `smb.conf`-Parameter ldap replication sleep eingeführt.)

Mögliche PDC/BDC-plus-LDAP-Konfigurationen beinhalten:

- PDC+BDC -> Ein zentraler LDAP-Server
- PDC -> LDAP-Master-Server, BDC -> LDAP-Slave-Server
- PDC -> LDAP-Master mit einem sekundären Slave-LDAP-Server

  BDC -> LDAP-Master mit einem sekundären Slave-LDAP-Server
- PDC -> LDAP-Master mit einem sekundären Slave-LDAP-Server

  BDC -> LDAP-Slave-Server mit einem sekundären Master-LDAP-Server

Um eine so genannte Fall-Back-Konfiguration zu haben (sekundärer LDAP-Server), würde man den sekundären LDAP-Server in der Datei `smb.conf` so angeben wie in Beispiel 6.2.2.

Beispiel 6.2.2. Mehrere LDAP-Server in smb.conf

```
...
        passdb backend =
ldapsam:ldap://master.quenya.org ldap://slave.quenya.org"
...
```

6.2.3 Domänen-Verwaltung mit Active-Directory

Seit der Veröffentlichung von MS Windows 2000 und Active Directory werden diese Informationen nun in einem Verzeichnis abgelegt, das repliziert werden kann und für das die Administration teilweise oder vollständig delegiert werden kann. Samba-3 kann NICHT Domänencontroller innerhalb eines Active-Directory-Baums sein und es kann NICHT ein Active-Directory-Server sein. Das bedeutet, dass Samba-3 auch NICHT als BDC für einen Active-Directory-DC arbeiten kann.

6.2.4 Was zeichnet einen Domänencontroller im Netzwerk aus?

Jede Maschine, die DC für die Domäne MITTELERDE ist, muss den NetBIOS-Gruppen-Namen MITTELERDE<#1c> am WINS-Server registrieren und/oder diesen Namen im LAN per Broadcast verteilen. Der PDC registriert zusätzlich den eindeutigen NetBIOS-Namen MITTELERDE<#1b> am WINS-Server. Der Namenstyp <#1b> ist normalerweise für den Domänen-Master-Browser reserviert, eine Rolle, die nichts mit irgendetwas in Bezug auf Authentifikation zu tun hat; aber die Microsoft-Domänen-Implementation verlangt, dass der Domänen-Master-Browser auf derselben Maschine läuft wie der PDC.

Wo kein WINS-Server verwendet wird, müssen Namensregistrierungen mittels Broadcast reichen. In Abschnitt 10.3 finden Sie mehr Informationen zu TCP/IP-Netzwerk-Protokollen und dazu, wie SMB/CIFS-Namen verwendet werden.

6.2.5 Wie findet eine Workstation ihren Domänencontroller?

Es gibt zwei unterschiedliche Mechanismen, um einen DC zu finden. Je nachdem, ob NetBIOS über TCP/IP aktiviert ist oder nicht, wird die eine oder andere Methode verwendet.

Wenn NetBIOS über TCP/IP deaktiviert ist, beinhaltet jegliche Namensauflösung die Verwendung von DNS, von Broadcasts über UDP und der ADS-Kommunikationstechnologie. In einer solchen Umgebung brauchen alle Maschinen entsprechene DNS-Einträge. Mehr dazu erfahren Sie in Abschnitt 10.3.3.

6.2.5.1 NetBIOS über TCP/IP aktiviert

Eine MS Windows NT4/200x/XP Professional-Workstation in der Domäne MITTELERDE, die einen lokalen Benutzer authentifizieren will, muss den DC für MITTELERDE finden.

Sie macht das über eine NetBIOS-Namens-Abfrage für den Gruppen-Namen MITTELER-DE<#1c>. Die Workstation geht davon aus, dass jede Maschine, die auf diese Anfrage antwortet, ein DC ist und Anmelde-Anfragen beantworten kann. Um keine Sicherheitslücken zu öffnen, authentifizieren die Workstation und der gewählte DC einander gegenseitig. Danach sendet die Workstation die Benutzerdaten (Name/Passwort) zur Überprüfung an den lokalen DC.

6.2.5.2 NetBIOS über TCP/IP deaktiviert

Eine MS Windows NT4/200x/XP Professional-Workstation in dem Realm `quenya.org`, die die Benutzer-Authentifikation beeinflussen will, wird den DC dadurch ausfindig machen, dass sie DNS-Server nach dem Eintrag `_ldap._tcp.pdc.ms-dcs.quenya.org` abfragt. Mehr Informationen zu diesem Thema finden Sie in Abschnitt 10.3.3.

6.3 Konfiguration eines Backup-Domänen-Controllers

Das Einrichten eines BDCs erfordert einige Schritte, um den Samba-Server vor der ersten Ausführung von smbd vorzubereiten. Diese Schritte sind die folgenden:

- Die Domänen-SID muss auf dem PDC und dem BDC gleich sein. In Samba-Versionen vor 2.2.5 wurde die SID in der Datei `private/MACHINE.SID` gespeichert. Jetzt wird die Domänen-SID in der Datei `private/secrets.tdb` gespeichert. Diese Datei ist einzigartig für jeden Server und kann nicht vom PDC auf den BDC kopiert werden; der BDC wird bei jedem Start eine neue SID generieren. Er wird die Domänen-SID des PDC mit der neu angelegten BDC-SID überschreiben. Es gibt eine Prozedur, die es dem BDC erlaubt, die Domänen-SID zu beziehen. Diese wird hier beschrieben.

  Um die Domänen-SID vom PDC oder einem existenten BDC zu beziehen und sie in `secrets.tdb` zu speichern, führen Sie Folgendes aus:

  ```
  root# net rpc getsid
  ```

- Die Spezifikation der Option ldap admin dn ist zwingend. Dies erfordert, dass das LDAP-Administrationspasswort in `secrets.tdb` mit **smbpasswd -w** *mysecret* gesetzt wird.

- Es muss entweder ldap suffix oder ldap idmap suffix in der Datei `smb.conf` angegeben werden.

- Die UNIX-Benutzer-Datenbank muss vom PDC auf den BDC synchronisiert werden. Dies bedeutet, dass sowohl `/etc/passwd` als auch `/etc/group` vom PDC auf den BDC repliziert werden müssen. Dies kann manuell geschehen, wenn immer Veränderungen vorgenommen werden. Alternativ kann der PDC als NIS-Master-Server und der BDC als NIS-Slave-Server angelegt werden. Den BDC als reinen NIS-Client aufzusetzen wäre nicht genug, da der BDC nicht auf seine Benutzer-Datenbank zugreifen kann, sollte der PDC ausfallen. NIS ist auf keinen Fall der einzige Weg, um Passwörter zu synchronisieren. Eine Lösung mit LDAP würde genauso funktionieren.

- Die Samba-Passwort-Datenbank muss vom PDC auf den BDC repliziert werden. Obwohl es möglich ist, die Datei `smbpasswd` mit dem Befehlen **rsync** und **ssh** zu synchronisieren, ist diese Methode unbrauchbar und fehlerhaft und wird daher nicht empfohlen. Eine bessere Lösung ist es, Slave-LDAP-Server für jeden BDC, und einen Master-LDAP-Server für den PDC aufzusetzen.
- Die netlogon-Freigabe muss vom PDC auf den BDC repliziert werden. Dies kann manuell geschehen, wenn Veränderungen vorgenommen werden, oder es kann automatisch geschehen, mit Hilfe eines **cron**-Jobs, der die Verzeichnisstruktur in dieser Freigabe mit einem Werkzeug wie **rsync** repliziert.

6.3.1 Beispielkonfiguration

Schlussendlich muss der BDC von den Workstations gefunden werden. Dazu konfigurieren Sie Samba, wie in Beispiel 6.3.1 gezeigt ist.

Beispiel 6.3.1. Minimales Setup für einen BDC

```
workgroup = MITTELERDE
passdb backend = ldapsam:ldap://slave-ldap.quenya.org
domain master = no
domain logons = yes
idmap backend = ldap:ldap://slave-ldap.quenya.org
```

Diese Einträge nehmen Sie im Abschnitt *[global]* von `smb.conf` des BDCs vor. Dies veranlasst den BDC, nur den Namen SAMBA<#1c> am WINS-Server zu registrieren. Das ist kein Problem, da der Name SAMBA<#1c> ein NetBIOS-Gruppen-Name ist, der von mehreren Maschinen registriert werden soll. Der Parameter domain master = no zwingt den BDC dazu,
SAMBA<#1b> nicht zu registrieren, der als einzigartiger NetBIOS-Name für den PDC reserviert ist.

Der Parameter *idmap backend* wird das Werkzeug **winbindd** dazu veranlassen, die LDAP-Datenbank zur Auflösung aller UIDs und GIDs für UNIX-Konten zu verwenden.

Anmerkung

Samba-3 hat eine neue Möglichkeit eingeführt, IDs zu „*mappen*“. Diese erlaubt unter anderem eine größere Flexibilität im Umgang mit UIDs und GIDs in Bezug auf NT-Domänen-User- und Gruppen-SIDs. Eine der neuen Funktionalitäten gewährleistet explizit, dass UNIX/Linux-UIDs und -GIDs konsistent auf dem PDC, allen BDCs und allen Domänen-Mitgliedsservern sind. Der Parameter, der dies kontrolliert, heißt *idmap backend*. Bitte konsultieren Sie die Manpage zu `smb.conf` für mehr Informationen zu seinem Verhalten.

Die Verwendung der Option idmap backend = ldap:ldap://master.quenya/org auf einem BDC macht nur Sinn, wenn ldapsam auf einem PDC eingesetzt wird. Der Zweck eines auf LDAP basierenden idmap-Backends ist es, einem Domänen-Mitglied (das kein eigenes passdb-Backend hat) die Verwendung von winbindd zu gestatten, um Windows-Netzwerk-Benutzer und -Gruppen zu UID/GIDs aufzulösen. Anders gesagt: Diese Option ist für die Verwendung auf Domänen-Mitgliedsservern gedacht.

6.4 Häufige Fehler

Da dies ein ziemlich neues Feld für Samba ist, gibt es noch nicht allzu viele Beispiele, auf die wir verweisen können. Updates werden veröffentlicht werden, sobald sie verfügbar werden, und können in zukünftigen Samba-Releases oder auf der Samba-Website <`http://samba.org`> gefunden werden.

6.4.1 Maschinen-Konten laufen immer wieder ab

Dieses Problem tritt auf, wenn die passdb-Dateien (SAM) von einem zentralen Server aus kopiert werden, aber der lokale BDC als PDC arbeitet. Dies führt zu Updates der Passwörter der lokalen Maschinen-Vertrauenskonten in der lokalen SAM. Solche Updates werden nicht zum zentralen Server zurückkopiert. Das neuere Maschinen-Konten-Passwort wird damit überschrieben, sobald die SAM vom PDC neu kopiert wird. Das Ergebnis ist, dass die Domänen-Mitgliedsmaschine beim Start keine Übereinstimmung zwischen ihren eigenen Passwörtern und denen in der Datenbank findet, und da der Sicherheits-Check beim Start daher fehlschlägt, wird diese Maschine keine Anmelde-Versuche zulassen und es wird der Fehler gemeldet, dass das Konto abgelaufen ist.

Die Lösung ist, ein robusteres passdb-Backend zu verwenden, wie z.B. das ldapsam-Backend, und mit diesem für jeden BDC einen Slave-LDAP-Server aufzusetzen sowie einen Master-LDAP-Server für den PDC.

6.4.2 Kann Samba ein BDC für einen NT4-PDC sein?

Nein. Die nativen NT4-SAM-Replikationsprotokolle wurden noch nicht vollständig implementiert.

Kann ich die Vorteile eines BDCs mit Samba nutzen? Ja, jedoch nur mit einem Samba-PDC. Das Hauptargument zur Einrichtung eines BDCs ist die gesteigerte Verfügbarkeit. Wenn der PDC ein Samba-Host ist, kann ein zweiter Samba-Host aufgesetzt werden, um Anmelde-Anfragen zu behandeln, wenn der PDC nicht verfügbar ist.

6.4.3 Wie repliziere ich die Datei smbpasswd?

Die Replikation der Datei smbpasswd ist eine sehr empfindliche Angelegenheit. Sie muss geschehen, wann immer Änderungen an der SAM durchgeführt werden. Die Passwort-Änderungen jeden Benutzers werden in der smbpasswd durchgeführt und müssen auf den BDC repliziert werden. Daher ist die Replikation sehr oft notwendig.

Da die Datei smbpasswd Klartext-Passwort-Äquivalente enthält, darf sie nicht unverschlüsselt über das Netz versandt werden. Die beste Art der smbpasswd-Replikation ist die Verwendung des Werkzeugs rsync. rsync kann ssh als Transport-Tunnel nutzen. **ssh** selbst kann wiederum so konfiguriert werden, dass es *only*-Transfers mittels **rsync** erlaubt, ohne vom Benutzer die Eingabe eines Passworts zu verlangen.

Wie bereits einige Male zuvor erwähnt wurde, ist diese Methode fehlerhaft und unvollständig. DIe Synchronisation der Maschinen-Vertrauenskonten gerät aus dem Tritt, was in einer unbrauchbaren Domäne resultiert. Diese Methode wird *nicht* empfohlen. Verwenden Sie stattdessen LDAP.

6.4.4 Kann ich all dies mit LDAP erledigen?

Die einfache Antwort lautet: Ja. Der pdb_ldap-Code von Samba ermöglicht es, sich mit einem Replika-LDAP-Server zu verbinden, und folgt außerdem Referrals und Rebinds zum Master, wann immer Samba Änderungen an der Datenbank vornehmen muss. (Normalerweise sind BDCs read-only, daher wird dies nicht oft vorkommen).

Kapitel 7

DOMÄNEN-MITGLIEDSCHAFT

Domänen-Mitgliedschaft ist ein Thema von regem Interesse. Samba muss fähig sein, als ein Mitgliedsserver in einem Microsoft-Domänen-Sicherheitskontext teilzunehmen, und Samba muss fähig sein, Maschinen-Vertrauenskonten für Domänen-Maschinen anzubieten; anderenfalls wäre es keine erwägenswerte Option für viele Anwender.

Dieses Kapitel umfasst Hintergrund-Informationen zur Domänen-Mitgliedschaft, zu der dazu notwendigen Samba-Konfiguration und zu MS-Windows-Client-Prozeduren zum Beitreten zu einer Domäne. Warum dies notwendig ist? Weil in beiden Bereichen sowohl in der MS-Windows-Netzwerk-Welt als auch insbesondere in der UNIX/Linux- Netzwerk- und Administrationswelt ein bemerkenswertes Maß an Uninformiertheit, falschen Vorstellungen und fehlendem Wissen existiert. Es ist zu hoffen, dass dieses Kapitel die Lücken füllt.

7.1 Eigenschaften und Vorzüge

MS-Windows-Workstations und -Server, die an der Domänen-Sicherheit teilhaben wollen, müssen zu Domänen-Mitgliedern gemacht werden. Das Teilnehmen an der Domänen-Sicherheit wird oft *Single Sign On* oder kurz SSO genannt. Dieses Kapitel beschreibt den Prozess, der durchgeführt werden muss, um eine Workstation (oder einen anderen Server, z.B. einen MS Windows NT4/200x- Server) oder einen Samba-Server zu einem Mitglied in einem Microsoft-Domänen-Sicherheitskontext zu machen.

Samba-3 kann sich einer MS-Windows-artigen Domäne als nativer Mitgliedsserver anschließen oder einem Samba-kontrollierten Netzwerk. Domänen-Mitgliedschaft hat viele Vorteile:

- MS-Windows-Workstation-Benutzer erhalten die Vorteile von SSO.
- Zugriffsrechte von Domänen-Benutzern und Datei-Benutzer/Zugriffs-Kontrollen können über die einzelne „*Domain Security Account Manager*“-(SAM-)Datenbank gesetzt werden. (Sie arbeitet genauso mit Domänen-Mitgliedsservern wie auch mit MS-Windows-Workstations, die Domänen-Mitglieder sind.)
- Nur MS Windows NT4/200x/XP Professional-Workstations, die Domänen-Mitglieder sind, können Netzwerk-Anmeldedienste benutzen.
- Domänen-Mitglieds-Workstations können durch die Verwendung von Policy-Dateien (`NTConfig.POL`) und Desktop-Profilen besser kontrolliert werden.

- Durch die Verwendung von Anmelde-Skripts können Benutzer transparenten Zugriff auf Netz-Anwendungen erhalten, die auf Applikationsservern laufen.
- Netzwerk-Administratoren erhalten bessere Möglichkeiten zum Management von Applikations- und Benutzer-Zugriffen, da kein Bedarf mehr besteht, Benutzer-Konten auf irgendeinem Netzwerk-Client oder -Server zu verwalten, außer in der zentralen Domänen-Datenbank. (Diese ist entweder NT4/Samba-SAM-artig, eine NT4-Domäne, die durch ein LDAP-Backend ergänzt wird, oder eine Active-Directory-Infrastruktur.)

7.2 Maschinen-Vertrauenskonten mit MS Windows Workstations bzw. Servern

Ein Maschinen-Vertrauenskonto ist ein Konto, das dazu verwendet wird, eine Client-Maschine (und nicht einen Benutzer) am Domänen-Controller zu authentifizieren. In der Windows- Terminologie ist dies als „*Maschinen-Konto*“ bekannt. Der Zweck des Maschinen-Kontos ist es zu verhindern, dass ein böswilliger Benutzer einen Domänen-Controller missbraucht, um Zugriff auf eine Domänen-Mitglieds-Workstation zu erhalten.

Das Passwort eines Maschinen-Vertrauenskontos fungiert als „*gemeinsames Geheimnis*“ für die sichere Kommunikation mit dem Domänencontroller. Dies ist ein Sicherheits-Feature, um eine nicht autorisierte Maschine mit demselben NetBIOS-Namen davon abzuhalten, sich der Domäne anzuschließen und Zugriff auf Benutzer/Gruppen-Konten der Domäne zu erhalten. Windows NT/200x/XP Professional-Clients nutzen Maschinen-Vertrauenskonten, aber Windows 9x/Me/XP Home-Clients tun das nicht. Daher ist ein Windows 9x/Me/XP Home-Client nie ein vollwertiges Domänen-Mitglied, da er kein Maschinen-Vertrauenskonto besitzt und auf diese Weise kein „*gemeinsames Geheimnis*“ mit dem Domänencontroller teilt.

Ein Windows NT4-PDC speichert jedes Maschinen-Vertrauenskonto in der Windows-Registrierung. Die Einführung von MS Windows 2000 brachte auch die Einführung des Active Directory, dem neuen Repository für Maschinen-Vertrauenskonten. Ein Samba-PDC speichert jedoch jedes Maschinen-Vertrauenskonto in zwei Teilen, und zwar wie folgt:

- In einem Domänen-Sicherheits-Konto (gespeichert in dem passdb backend, das in der Datei `smb.conf` konfiguriert wurde. Die exakte Form der gespeicherten Konten-Information ist vom Typ des gewählten Backends abhängig.

  Das ältere Format dieser Daten ist die Datenbank `smbpasswd`, die die UNIX-Login-ID, den UNIX user identifier (UID), die LanMan- und die verschlüsselten NT-Passwörter enthält. Es gibt noch weitere Informationen zu dieser Datei, die uns jedoch an dieser Stelle nicht interessieren.

  Die zwei neueren Datenbank-Typen heißen ldapsam und tdbsam. Beide speichern bei weitem mehr Daten als das ältere `smbpasswd`. Die zusätzlichen Informationen ermöglichen das Implementieren neuer Funktionen für Benutzer-Konten.

- In einem entsprechenden UNIX-Konto, das meist in `/etc/passwd` gespeichert wird.

Es gibt drei Möglichkeiten, Maschinen-Vertrauenskonten anzulegen:

- Manuelles Anlegen auf der UNIX/Linux-Befehlszeile. Hier werden sowohl das Samba- als auch das zugehörige UNIX-Konto von Hand angelegt.

- Das Verwenden von MS Windows NT4 Server Manager, entweder auf einem NT4 Domain Member Server oder unter Verwendung des Nexus-Toolkits, das auf der Microsoft-Website verfügbar ist. Dieses Tool kann von jeder MS Windows-Maschine aus verwendet werden, solange der Benutzer als Administrator angemeldet ist.
- „*On-the-fly*“ anlegen. Das Samba-Maschinen-Vertrauenskonto wird automatisch von Samba angelegt, wenn sich der Client der Domäne anschließt. (Aus Sicherheitsgründen ist dies die empfohlene Methode.) Das zugehörige UNIX-Konto kann automatisch oder manuell angelegt werden.

7.2.1 Manuelles Anlegen von Maschinen-Vertrauenskonten

Der erste Schritt beim manuellen Anlegen eines Maschinen-Vertrauenskontos ist das manuelle Anlegen des zugehörigen UNIX-Kontos in der Datei `/etc/passwd`. Dies kann mit **vipw** oder einem anderen „*add user*“-Befehl geschehen, der normalerweise zum Anlegen von UNIX-Benutzern verwendet wird. Hier ein Beispiel für einen Linux-basierenden Samba-Server:

```
root# /usr/sbin/useradd -g machines -d /dev/null -c "machine nickname" \
   -s /bin/false machine_name$

root# passwd -l machine_name$
```

Im obigen Beispiel gibt es eine System-Gruppe „*machines*“, die als primäre Gruppe für alle Maschinen-Konten verwendet wird. In den folgenden Beispielen hat die Gruppe „*machines*“ eine numerische GID von 100.

Auf *BSD-Systemen kann dies mit dem Utility **chpass** geschehen:

```
root# chpass -a \
'machine_name$:*:101:100::0:0:Windows machine_name:/dev/null:/sbin/nologin'
```

Der Eintrag in `/etc/passwd` wird den Maschinen-Namen enthalten, mit einem angefügten „*$*“, ohne Passwort, mit einer Null-Shell und ohne home-Verzeichnis. Zum Beispiel würde eine Maschine namens „*doppy*“ diesen Eintrag haben:

```
doppy$:x:505:100:machine_nickname:/dev/null:/bin/false
```

Im obigen Beispiel kann *machine_nickname* eine beliebige Beschreibung des Clients sein, z.B. RechnerSekretariat. *machine_name* muss definitiv der NetBIOS-Name des Clients sein, der zu der Domäne hinzugefügt werden soll. Das Zeichen „*$*“ muss an den NetBIOS-Namen des Clients angefügt werden, oder Samba wird dieses Konto nicht als Maschinen-Vertrauenskonto erkennen.

Jetzt, wo das zugehörige UNIX-Konto angelegt worden ist, besteht der nächste Schritt im Anlegen des Samba-Kontos für den Client. Das Konto enthält das wohlbekannte ur-

sprüngliche Passwort des Maschinen-Vertrauenskontos. Dies kann mit dem Befehl **smbpasswd** geschehen, wie hier gezeigt:

```
root# smbpasswd -a -m machine_name
```

wobei *machine_name* der NetBIOS-Namen der Maschine ist. Die RID des neuen Maschinen-Kontos wird aus der UID des zugehörigen UNIX-Kontos generiert.

SCHLIESSEN SIE DEN CLIENT UNVERZÜGLICH DER DOMÄNE AN

Das manuelle Anlegen eines Maschinen-Vertrauenskontos mit dieser Methode entspricht dem Anlegen eines Maschinen-Vertrauenskontos auf einem Windows NT-PDC mit dem Server Manager. Vom Zeitpunkt des Anlegens des Kontos bis zum Anschließen des Clients an die Domäne und zum Ändern des Passworts ist Ihre Domäne durch Eindringlinge bedroht, die sich mit einer Maschine mit dem gleichen NetBIOS-Namen der Domäne anschließen. Ein PDC vertraut Mitgliedern der Domäne und wird eine große Menge Benutzer-Informationen an solche Clients weitergeben. Sie wurden gewarnt!

7.2.2 Das Verwalten von Domänen-Maschinen-Konten mit dem Server Manager

Ein funktionierendes add machine script-Skript ist unbedingt notwendig, um Maschinen-Vertrauenskonten automatisch anlegen zu können. Dies gilt unabhängig davon, ob man das automatische Anlegen der Konten verwendet oder den NT4 Domain Server Manager.

Wenn die Maschine, von der aus Sie versuchen, die Domäne zu verwalten, eine MS Windows NT4 Workstation oder MS Windows 200x/XP Professional ist, müssen Sie als Werkzeug das Package namens **SRVTOOLS.EXE** wählen. Wenn es im Zielverzeichnis ausgeführt wird, entpackt es **SrvMgr.exe** und **UsrMgr.exe**. Beides sind Domänen-Management-Werkzeuge für MS Windows NT4 Workstation.

Wenn Ihre Workstation ein Produkt der Microsoft Windows 9x/Me-Familie ist, sollten Sie das Package **Nexus.exe** von der Microsoft-Website laden. Auch dies wird dieselben Tools entpacken, aber eben für die Windows 9x/Me-Plattformen.

Weitere Informationen zu diesen Tools können Sie von folgenden Stellen beziehen:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;173673>
<http://support.microsoft.com/default.aspx?scid=kb;en-us;172540>

Starten Sie **srvmgr.exe** (Server Manager für Domänen), und folgen Sie diesen Schritten: Verwaltung von Maschinen-Konten mittels Server Manager

1. Wählen Sie den Eintrag **Computer** aus dem Menü.

2. Klicken Sie auf **Select Domain**.
3. Klicken Sie im Panel **Select Domain** auf den Namen der Domäne, die Sie administrieren wollen, und dann auf **OK**.
4. Wählen Sie nochmals das Menü **Computer**.
5. Wählen Sie **Add to Domain**.
6. Klicken Sie auf den Radio-Button **Add NT Workstation of Server** in der folgenden Dialogbox, geben Sie den Maschinen-Namen im vorgegebenen Feld ein, und klicken Sie auf **Add**.

7.2.3 „*On-the-Fly*"-Anlegen von Maschinen-Konten

Die zweite (und empfohlene) Art, Maschinenkonten anzulegen, besteht darin, es einfach dem Samba-Server zu erlauben, diese Konten bei Bedarf anzulegen, wenn der Client der Domäne angeschlossen wird.

Da jedes Maschinen-Vertrauenskonto unter Samba ein zugehöriges UNIX-Konto benötigt, wird üblicherweise eine Methode zum automatischen Anlegen eines UNIX-Kontos bereitgestellt; dies erfordert die Konfiguration der Option „*add machine script*" in der Datei `smb.conf`. Diese Methode ist jedoch nicht erforderlich, die benötigten UNIX-Konten können auch von Hand angelegt werden.

Hier ein Beispiel für ein Red Hat Linux-System.

```
[global]
# <...Erinnerung an Parameter...>
        add machine script = /usr/sbin/useradd -d /dev/null -g 100 \
-s /bin/false -M %u
```

7.2.4 Eine MS Windows-Workstation oder einen MS Windows-Server zum Domänen-Mitglied machen

Die Vorgehensweise, wie Sie eine MS Windows-Workstation oder einen MS Windows-Server zum Domänen-Mitglied machen, hängt von der Version von Windows ab.

7.2.4.1 Windows 200x/XP Professional-Client

Wenn der Benutzer den Client dazu „*auserwählt*", ein Domänen-Mitglied zu werden, fragt Windows 200x nach einer Konto/Passwort-Kombination, die dazu berechtigt ist, Maschinen-Konten in der Domäne anzulegen. Ein Samba-Administrator-Konto (also ein Samba-Konto, das `root`-Rechte auf dem Samba-Server hat) muss hier verwendet werden; der Vorgang wird scheitern, wenn ein normales Benutzerkonto verwendet wird.

Aus Sicherheitsgründen sollte das Passwort für dieses Administrator-Konto auf ein anderes Passwort gesetzt werden als jenes, das für den Benutzer root in `/etc/passwd` verwendet wird.

Der Name des Kontos, das zum Anlegen von Domänenmitglieds-Maschinen-Konten verwendet wird, kann etwas Beliebiges sein, das der Netzwerk-Administrator wählt. Wenn dieser Name etwas anderes als `root` ist, wird er einfach auf den dem Benutzer `root` zugehörigen Eintrag in der Datei „*gemappt*“, die vom Parameter username map = /etc/samba/smbusers in der Datei `smb.conf` bezeichnet wird.

Der „*Session-Key*“ des Samba-Administrator-Kontos fungiert als Verschlüsselungsschlüssel zum Setzen des Passworts für das Maschinen-Vertrauenskonto. Das Maschinen-Vertrauenskonto wird on-the-fly angelegt oder aktualisiert, falls es bereits existiert.

7.2.4.2 Windows NT4-Client

Wenn das Maschinen-Vertrauenskonto manuell angelegt wurde, geben Sie im Menü „*Identification Changes*“ den Domänen-Namen an, aber aktivieren Sie NICHT die Box **Create a Computer Account in the Domain**. In diesem Fall wird das bereits existierende Maschinen-Vertrauenskonto verwendet, um die Maschine an die Domäne anzuschließen.

Wenn das Maschinen-Vertrauenskonto on-the-fly angelegt werden soll, geben Sie im Menü „*Identification Changes*“ den Domänen-Namen an und aktivieren die Box **Create a Computer Account in the Domain**. In diesem Fall wird der Anschluss an die Domäne wie oben für Windows 2000 beschrieben fortgesetzt (d.h., Sie müssen ein Samba-Administrator-Konto angeben, wenn danach verlangt wird).

7.2.4.3 Samba-Client

Das Anschließen eines Samba-Clients an eine Domäne wird in Domänen-Mitgliedsserver beschrieben.

7.3 Domänen-Mitgliedsserver

Diese Server-Betriebsart beinhaltet, dass die Samba-Maschine zum Domänen-Mitglied gemacht wird. Das bedeutet per Definition, dass jegliche Benutzer-Authentifikation durch ein zentral bestimmtes Authentifikationsregime erfolgen wird. Das Authentifikationsregime kann von einem NT3/4-artigen (alte Domänen-Technologie) Server kommen, oder es kann von einem Active Directory Server (ADS) bereitgestellt werden, der unter MS Windows 2000 oder einem neueren MS Windows läuft.

Es sollte natürlich klar sein, dass das Authentifikations-Backend selbst ein Server von jeder Verzeichnis-Dienst-Architektur sein kann, die von Samba unterstützt wird. Es kann LDAP (von OpenLDAP) sein, oder iPlanet von Sun, ein NetWare Directory Server und so weiter.

Anmerkung

Wenn Samba für die Verwendung von LDAP konfiguriert ist (oder für eine andere Identitätsverwaltung und/oder einen Verzeichnisdienst), dann ist es Samba, das die Authentifikation von Benutzern und Maschinen weiter ausführt. Es sollte beachtet werden, dass der LDAP-Server die Authentifikation nicht anstelle von Samba ausführt.

Bitte besuchen Sie Domain Control für mehr Informationen darüber, wie man ein Domänen-Maschinen-Konto anlegt. Sie erfahren dort auch, wie man eine Samba-Maschine, die Domänen-Mitglied ist, dazu befähigt, sich der Domäne anzuschließen und deren volles Vertrauen zu gewinnen ...

7.3.1 Sich mit Samba-3 einer NT4-Domäne anschließen

Die nächste Tabelle enthält eine Liste von Namen, die im Rest dieses Kapitels verwendet wurden.

Tabelle 7.1. Annahmen

NetBIOS-Namen:	SERV1
Windows 200x/NT-Domänen-Namen:	MITTELERDE
NetBIOS-Namen des Domänen-PDC:	DOMPDC
NetBIOS-Namen der Domänen-BDCs:	DOMBDC1 und DOMBDC2

Als Erstes müssen Sie Ihre Datei `smb.conf` editieren, um Samba mitzuteilen, dass es ab jetzt Domänen-Sicherheit verwenden soll.

Ändern Sie die Zeile (oder fügen Sie sie hinzu) security im Abschnitt [global] Ihrer `smb.conf` auf:

```
security = domain
```

Als Nächstes ändern Sie die Zeile workgroup im Abschnitt *[global]* auf:

```
workgroup = MITTELERDE
```

Dies ist der Name der Domäne, der wir uns anschließen.

Sie müssen auch den Parameter encrypt passwords auf `yes` setzen, um Ihren Benutzern die Authentifikation am NT-PDC zu ermöglichen. Dies ist die Standard-Einstellung, falls dieser Parameter nicht gesetzt wird. Es gibt keinen Grund, diesen Parameter zu setzen, aber wenn er in der Datei `smb.conf` gesetzt wird, muss er auf `Yes` gesetzt werden.

Zuletzt fügen Sie dem Abschnitt [global] die Zeile password server hinzu (oder ändern sie), sodass sie wie folgt lautet:

```
password server = DOMPDC DOMBDC1 DOMBDC2
```

Dies sind der PDC und die BDCs, die Samba kontaktieren wird, um Benutzer zu authentifizieren. Samba wird versuchen, jeden dieser Server in der angegebenen Reihenfolge zu

kontaktieren, daher können Sie durch die Reihung der Server die Last auf die einzelnen Domänencontroller verteilen.

Wenn Sie andererseits wollen, dass smbd automatisch die Liste der zu verwendenden Domänencontroller bestimmt, können Sie diese Zeile auf Folgendes setzen:

*password server = **

Diese Methode erlaubt es Samba, genau denselben Mechanismus wie NT zu verwenden. Sie verwendet entweder Namensauflösung, die auf Broadcasts basiert, führt eine WINS-Datenbank-Abfrage durch, um einen Domänencontroller zu finden, oder lokalisiert einen Domänencontroller mittels DNS-Namensauflösung.

Zum Anschluss an eine Domäne geben Sie diesen Befehl:

```
root# net join -S DOMPDC -UAdministrator%Passwort
```

Wenn das Argument `-S DOMPDC` nicht angegeben wird, wird der Domänen-Name aus der Datei `smb.conf` gelesen.

Die Maschine schließt sich der Domäne DOM an, und der PDC für diese Domäne (die einzige Maschine, die Schreibzugriff auf die SAM-Datenbank der Domäne hat) ist DOMPDC, daher benutzen Sie die Option `-S`. *Administrator%Passwort* ist das Benutzer/Passwort-Paar für ein Konto, das die nötigen Privilegien hat, um Maschinen der Domäne hinzuzufügen. Wenn dies erfolgreich ist, werden Sie eine Nachricht in Ihrem Terminal-Fenster sehen, die den unten gezeigten Text enthält. Wo alte NT4-artige Domänen-Architektur eingesetzt wird, lautet sie:

```
Joined domain DOM.
```

Wo Active Directory eingesetzt wird, lautet sie:

```
Joined SERV1 to realm MYREALM.
```

Lesen Sie die **net**-Manpage für mehr Informationen.

Dieser Prozess schließt den Server an die Domäne an, ohne davor das Maschinen-Konto auf dem PDC anlegen zu müssen.

Dieser Befehl durchläuft das Protokoll zum Ändern des Maschinen-Konto-Passworts, dann schreibt er das neue (zufällige) Maschinen-Konto-Passwort für diesen Samba-Server in eine Datei in demselben Verzeichnis, in dem normalerweise die Datei `smbpasswd` gespeichert würde:

```
/usr/local/samba/private/secrets.tdb
oder
/etc/samba/secrets.tdb.
```

Diese Datei wird von root angelegt, gehört root und ist nicht von einem anderen Benutzer lesbar. Sie ist der Schlüssel zur Domänen-Sicherheit Ihres Systems und sollte genauso umsichtig behandelt werden wie eine Shadow-Passwort-Datei.

Zuletzt starten Sie Ihre Samba-Daemonen neu und machen sich bereit für die Clients, die die neue Domänen-Sicherheit zu benutzen beginnen. Die Art, auf die Sie die Samba-Daemons neu starten, hängt von Ihrer Distribution ab, aber in den meisten Fällen wird Folgendes ausreichen:

```
root# /etc/init.d/samba restart
```

7.3.2 Warum ist dies besser als security = server?

Derzeit befreit die Domänen-Sicherheit in Samba Sie nicht von der Aufgabe, lokale UNIX-Benutzer anlegen zu müssen, um die Benutzer, die sich an Ihrem Server anmelden, zu repräsentieren. Das bedeutet: Wenn sich der Domänen-Benutzer `DOM\fred` an Ihrem Samba-Domänen-Server anmeldet, muss es einen lokalen UNIX-Benutzer fred geben, um diesen Benutzer im UNIX-Datei-System zu repräsentieren. Dies ähnelt dem früheren Samba-Betriebsmodus security = server, wo Samba die Authentifizierungsanfrage an einen Windows NT-Server weitergeleitet hat, genau wie es ein Windows-95- oder Windows-98-Server tun würde.

Lesen Sie das Kapitel Winbind: Verwendung von Domänen-Konten für Informationen darüber, wie ein System automatisch UNIX-UIDs und -GIDs an Windows NT-Domänen-Benutzer und -Gruppen zuweisen kann.

Der Vorteil der Domänen-Level-Security ist, dass die Authentifikation in der Domänen-Level-Security über den authentifizierten RPC-Channel läuft, und zwar in exakt derselben Art, wie sie ein NT-Server ausführen würde. Das bedeutet, dass Samba-Server nunmehr in genau derselben Art an Domänen-Vertrauensverhältnissen teilnehmen, wie es NT-Server tun (z.B. können Sie Samba-Server einer Ressourcen-Domäne hinzufügen, und die Authentifikation vom Ressourcen-Domänencontroller auf einen Konten-Domänen-PDC weiterleiten).

Zusätzlich dazu muss jeder Samba-Daemon bei gesetzter Option security = server eine Verbindung zum Authentifikationsserver offen halten, solange der Daemon läuft. Das kann die Ressourcen eines Microsoft NT-Servers stark belasten, und es kann passieren, dass er nicht genügend verfügbare Verbindungen öffnen kann. Mit security = domain verbinden sich die Samba-Daemons nur so lange mit dem PDC/BDC, wie es zum Authentifizieren des Benutzers nötig ist. Danach trennen sie die Verbindung und schonen damit die Ressourcen des PDCs.

Zuletzt führt das identische Verhalten zu einem NT-Server dazu, dass beim Authentifizieren am PDC der Samba-Server als Teil der Authentifikationsantwort Benutzer-Informationen wie die Benutzer-SID, die Liste der Gruppen, der er angehört, und so weiter erhält.

ANMERKUNG

Ein großer Teil dieses Dokuments wurde zuerst im Web-Magazin LinuxWorld <http://www.linuxworld.com> veröffentlicht, und zwar als Artikel <http://www.linuxworld.com/linuxworld/lw-1998-10/lw-10-samba.html> url="http://www.linuxworld.com/linuxworld/lw-1998-10/lw-10-samba.html" /> *Doing the NIS/NT Samba*.

7.4 Samba-ADS-Domänen-Mitgliedschaft

Dies ist eine knapp gefasste Anleitung für das Setup von Samba-3 mit Kerberos-Authentifikation an einem Windows 200x-KDC. Wir setzen voraus, dass Sie mit Kerberos vertraut sind.

7.4.1 Das Konfigurieren von smb.conf

Sie müssen zumindest die folgenden drei Optionen in `smb.conf` verwenden:

```
        realm = ihre.kerberos.realm
        security = ADS
# Der folgende Parameter muss nur gesetzt werden, wenn er vorhanden ist.
# Der Standard-Wert, wenn er nicht vorhanden ist, ist yes.
        encrypt passwords = yes
```

Falls Samba den entsprechenden ADS-Server nicht korrekt über den Realm-Namen identifizieren kann, verwenden Sie die Option password server in `smb.conf`: `password server = ihr.k`

ANMERKUNG

Sie brauchen *keine* smbpasswd-Datei, und ältere Clients werden so authentifiziert, als ob security = domain gesetzt wäre, obwohl es nicht schadet, und es Ihnen erlaubt, lokale Benutzer zu haben, die nicht in der Domäne sind.

7.4.2 Das Konfigurieren von /etc/krb5.conf

Sowohl mit MIT- als auch mit Heimdal-Kerberos ist es unnötig, `/etc/krb5.conf` zu konfigurieren, es kann sogar schädlich sein.

Microsoft Active Directory Server legen automatisch SRV-Einträge in der DNS-Zone *_kerberos.REALM.NAME* an, und zwar für jeden KDC in der Realm. Dies ist Teil des Installations- und Konfigurationsprozesses zum Anlegen einer Active-Directory-Domäne.

Die aktuellen KRB5-Libraries des MIT und von Heimdal prüfen beide standardmäßig auf SRV-Einträge, werden also automatisch die KDCs finden. Zusätzlich gilt, dass `krb5.conf` nur die Angabe eines einzelnen KDC erlaubt, sogar wenn es mehr als einen gibt. Die Verwendung von DNS-Lookups erlaubt es den KRB5-Libraries, jeden verfügbaren KDC zu verwenden.

Beim manuellen Konfigurieren von `krb5.conf` sieht die minimale Konfiguration so aus:

```
[libdefaults]
   default_realm = IHRE.KERBEROS.REALM

[realms]
   IHRE.KERBEROS.REALM = {
   kdc = ihr.kerberos.server
   }

[domain_realms]
   .kerberos.server = IHRE.KERBEROS.REALM
```

Bei der Verwendung von Heimdal-Versionen vor 0.6 sind folgende Einstellungen vorzunehmen:

```
[libdefaults]
   default_realm      = IHRE.KERBEROS.REALM
   default_etypes     = des-cbc-crc des-cbc-md5
   default_etypes_des = des-cbc-crc des-cbc-md5

[realms]
        IHRE.KERBEROS.REALM = {
        kdc = ihr.kerberos.server
   }

[domain_realms]
        .kerberos.server = IHRE.KERBEROS.REALM
```

Prüfen Sie Ihre Konfiguration mit `kinit` *BENUTZERNAME@REALM*, und stellen Sie sicher, dass Ihr Passwort vom Win2000-KDC akzeptiert wird.

Mit Heimdal-Versionen vor 0.6 können Sie nur neu in ADS angelegte Konten verwenden oder Konten, deren Passwörter nach der Migration geändert worden sind (bzw. im Falle des Kontos `Administrator` nach der Installation). Im Moment kann ein Windows 2003-KDC nur mit Heimdal-Versionen nach 0.6 verwendet werden (und ohne default_etypes in `krb5.conf`). Unglücklicherweise ist dieser gesamte Bereich noch immer in Veränderung begriffen.

ANMERKUNG

Die Realm muss in GROSSBUCHSTABEN angegeben werden, sonst erhalten Sie den Fehler „*Cannot find KDC for requested realm while getting initial credentials*“ (Kerberos ist case-sensitive!).

ANMERKUNG

Zwischen zwei Servern muss die Zeit synchronisiert werden. Sie erhalten „*kinit(v5): Clock skew too great while getting initial credentials*“, wenn die Zeitabweichung mehr als fünf Minuten beträgt.

Die Limits für die Zeitabweichung sind in den Kerberos-Protokollen konfigurierbar. Die Voreinstellung beträgt fünf Minuten.

Sie müssen auch sicherstellen, dass Sie einen Reverse-DNS-Lookup auf die IP-Adresse Ihres KDCs durchführen können. Außerdem muss der Name, auf den dieser Reverse-Lookup zeigt, entweder der NetBIOS-Name des KDCs (z.B. der Hostname ohne angehängte Domäne) sein, oder er kann der NetBIOS-Name, gefolgt von der Realm, sein.

Am leichtesten erreichen Sie dies, indem Sie einen Eintrag in `/etc/hosts` hinzufügen, der die IP-Adresse Ihres KDCs dessen NetBIOS-Namen zuordnet. Wenn Sie dies nicht korrekt erstellen, erhalten Sie einen local error, wenn Sie versuchen, sich der Realm anzuschließen.

Wenn Sie nur Kerberos-Support in smbclient wollen, können Sie direkt zu Testen mit smbclient springen. Die Abschnitte Anlegen des Maschinen-Kontos und Testen des Server-Setups werden nur benötigt, wenn Sie Kerberos-Support für smbd und winbindd brauchen.

7.4.3 Anlegen des Maschinen-Kontos

Als Benutzer mit Schreibzugriff auf das Samba-Verzeichnis (üblicherweise root) führen Sie Folgendes aus:

```
root#  net ads join -U Administrator%Passwort
```

Wenn Sie einen Windows-Client zum Mitglied einer ADS-Domäne innerhalb einer komplexen Organisation machen, wollen Sie vielleicht das Maschinen-Konto innerhalb einer bestimmten Organisationseinheit anlegen. Samba-3 erlaubt dies mit folgender Syntax:

```
root#  kinit Administrator@ihre.kerberos.REALM
```

```
root#  net ads join Organisations-Einheit
```

Zum Beispiel wollen Sie vielleicht das Maschinen-Konto innerhalb eines Containers namens „*Server*“ unterhalb des organisatorischen Verzeichnisses „*Computer\Geschäftsstelle\Abteilung*“ anlegen. Das tun Sie wie folgt:

```
root#  net ads join "Computer\Geschäftsstelle\Abteilung\Server"
```

7.4.3.1 Mögliche Fehler

ADS-Support nicht einkompiliert Samba muss rekonfiguriert (entfernen Sie config.cache) und danach neu kompiliert werden, nachdem die Kerberos-Libraries und Header-Dateien installiert wurden.

net ads join fragt nach dem Benutzernamen Sie müssen sich mit `kinit` *`BENUTZERNAME@REALM`* an der Domäne anmelden. *`BENUTZERNAME`* muss ein Benutzer sein, der berechtigt ist, Maschinen zur Domäne hinzuzufügen.

Nicht unterstützte Verschlüsselungs- oder Prüfsummen-Arten Stellen Sie sicher, dass die Datei `/etc/krb5.conf` für den Typ und die Version des installierten Kerberos korrekt konfiguriert ist.

7.4.4 Testen des Server-Setups

Wenn das Anschließen an die Domäne erfolgreich war, werden Sie ein neues Maschinen-Konto im Active Directory sehen, mit dem NetBIOS-Namen Ihres Samba-Servers (im „*Computer*“ -Folder unter „*Benutzer*“ und „*Computer*“).

Versuchen Sie auf einem Windows 2000-Client `net use * \\server\share`. Sie sollten mit Kerberos eingeloggt werden, ohne ein Passwort zu brauchen. Wenn dies scheitert, führen Sie `klist tickets` aus. Haben Sie ein Ticket für den Server bekommen? Hat es den Verschlüsselungstyp DES-CBC-MD5?

Anmerkung

Samba kann sowohl die DES-CBC-MD5-Verschlüsselung als auch das ARCFOUR-HMAC-MD5-Encoding verwenden.

7.4.5 Testen mit smbclient

Versuchen Sie, sich mit smbclient und Kerberos auf Ihrem Samba-Server an einem Win2000-Server oder einem Samba-Server anzumelden. Verwenden Sie smbclient wie gewohnt, aber geben Sie die Option `-k` an, um die Kerberos-Authentifikation zu wählen.

7.4.6 Bemerkungen

Sie müssen das Administrator-Passwort zumindest einmal nach der DC-Installation ändern, um die richtigen Verschlüsselungsarten zu installieren.

Windows 200x scheint die Parameter *_kerberos._udp* und *_ldap._tcp* nicht im standardmäßigen DNS-Setup zu installieren. Vielleicht wird dies in späteren Service-Packs bereinigt werden.

7.5 Gemeinsames Nutzen von UID-Zuweisungen unter Samba-Domänen-Mitgliedern

Samba weist UNIX-Benutzer und -Gruppen (gekennzeichnet durch UIDs und GIDs) auf Windows-Benutzer und Gruppen zu (gekennzeichnet durch SIDs). Diese Zuweisungen werden vom *idmap*-Subsystem von Samba vorgenommen.

In manchen Fällen ist es hilfreich, diese Zuweisungen unter Samba-Domänen-Mitgliedern zu teilen, damit die Zuweisung *name->id* auf allen Maschinen identisch ist. Dies kann im Speziellen benötigt werden, wenn man Dateien sowohl über CIFS als auch über NFS bereitstellt.

Um *LDAP* *ldap idmap suffix* zu verwenden, setzen Sie:

```
ldap idmap suffix = ou=Idmap,dc=quenya,dc=org
```

Lesen Sie den `smb.conf`-Manpage-Eintrag zum Parameter ldap idmap suffix für mehr Informationen dazu.

Vergessen Sie auch nicht, die Option ldap admin dn anzugeben, und sicherzustellen, dass das LDAP-Administrationspasswort in der Datei `secrets.tdb` gesetzt ist, indem Sie Folgendes ausführen:

```
root#  smbpasswd -w ldap-admin-passwort
```

7.6 Gängige Fehler

In dem Ablauf von Hinzufügen/Löschen/Wiederhinzufügen von Domänen-Maschinen-Konten gibt es viele Fallen für den unvorsichtigen Spieler und viele „*kleine*“ Dinge, die schief gehen können. Es ist besonders interessant, wie oft Teilnehmer der Samba-Mailing-Liste nach wiederholten gescheiterten Versuchen, ein Maschinen-Konto hinzuzufügen, den Schluss gezogen haben, dass es nötig sei, MS Windows auf der betreffenden Maschine „*neu zu installieren*“. In Wirklichkeit ist dies bei diesem Problem selten nötig. Die eigentliche Lösung ist oft ziemlich einfach, und das Problem lässt sich leicht beheben, wenn Sie verstehen, wie MS Windows-Netzwerke funktionieren.

7.6.1 Eine Maschine kann nicht noch einmal der Domäne hinzugefügt werden

„*Eine Windows-Workstation wurde neu installiert. Das Original-Maschinen-Konto wurde gelöscht und unmittelbar hinzugefügt. Die Workstation schließt sich der Domäne nicht an,*

wenn ich denselben Maschinen-Namen verwende. Meine Versuche, die Maschine hinzuzufügen, scheitern mit der Meldung, dass die Maschine bereits im Netzwerk existiert. Ich weiß, dass sie dies nicht tut. Warum scheitert dies?"

Der Original-Name ist nach wie vor im NetBIOS-Namens-Cache und muss erst ablaufen, nachdem das Maschinen-Konto gelöscht wurde, bevor man denselben Namen wieder als Domänen-Mitglied hinzufügen kann. Der beste Tipp dazu ist, das alte Konto zu löschen und dann die Maschine mit einem neuen Namen wieder hinzuzufügen.

7.6.2 Das Hinzufügen einer Maschine zur Domäne scheitert

„*Das Hinzufügen einer Windows 200x- oder XP Professional-Maschine zur Domäne scheitert mit der Meldung Der Computer konnte der Domäne nicht hinzugefügt werden,... Warum?*"

Sie sollten prüfen, dass es die Option add machine script in Ihrer Datei `smb.conf` gibt. Wenn es sie nicht gibt, fügen Sie bitte eine hinzu, die passend für Ihr Betriebssystem ist. Falls ein Skript definiert ist, werden Sie dessen Funktion prüfen müssen. Erhöhen Sie das log level in der `smb.conf`-Datei auf level 10, und versuchen Sie dann nochmals, sich der Domäne anzuschließen. Prüfen Sie die Log-Dateien, um zu sehen, welche Operation scheitert.

Mögliche Ursachen sind:

- Das Skript existiert nicht oder kann nicht in dem angegebenen Pfad gefunden werden.

  Korrektur: Fixen Sie es. Stellen Sie sicher, dass das Skript beim Ausführen von Hand sowohl das UNIX-Konto als auch das Samba-SAM-Konto anlegt.

- Die Maschine konnte nicht zur UNIX-Systemkonten-Datei `/etc/passwd` hinzugefügt werden.

  Korrektur: Überprüfen Sie, dass der Maschinenname ein gültiger UNIX-Systemkonten-Name ist. Wenn das UNIX-Werkzeug **useradd** aufgerufen wird, stellen Sie sicher, dass der Maschinen-Name, den Sie hinzufügen wollen, auch mit diesem Werkzeug hinzugefügt werden kann. Auf manchen Systemen erlaubt **useradd** keine Großbuchstaben oder Leerzeichen in dem Namen.

Das add machine script legt kein Maschinen-Konto in der Samba-Backend-Datenbank an, es ist nur dazu da, ein UNIX-System-Konto anzulegen, dem ein Samba-Backend-Datenbank-Konto zugewiesen werden kann.

7.6.3 Ich kann mich keinem Windows 2003-PDC anschließen

Windows 2003 erfordert ein SMB-Signing. Client-seitiges SMB-Signing wurde in Samba-3.0 implementiert. Setzen Sie client use spnego = yes, wenn Sie mit einem Windows 2003-Server kommunizieren.

Kapitel 8

STAND-ALONE-SERVER

Stand-alone-Server sind im Netzwerk unabhängig von Domänencontrollern. Sie sind keine Domänen-Mitglieder und funktionieren eher wie Arbeitsgruppen-Server. In vielen Fällen wird ein Stand-alone-Server mit einem Minimum an Sicherheitskontrolle konfiguriert, mit der Absicht, dass alle Daten für alle Benutzer frei zugänglich sein sollen.

8.1 Eigenschaften und Vorzüge

Stand-alone-Server können so sicher oder so unsicher gemacht werden, wie es die Anforderungen vorgeben. Sie können simple oder komplexe Konfigurationen haben. Generell, trotz all dem Trara um Domänen-Sicherheit, bleiben sie eine sehr gängige Installationsform.

Wenn alles, was gebraucht wird, ein Server mit Read-only-Dateien ist oder ein Server nur für Drucker, dann macht es keinen Sinn, eine komplexe Installation aufzusetzen. Zum Beispiel: Ein Zeichenbüro muss alte Zeichnungen und Referenz-Standard-Dateien speichern. Niemand kann Dateien auf den Server schreiben, da es gesetzlich vorgeschrieben ist, dass alle Dokumente unverändert bleiben. Ein Stand-alone-Server im Read-only-Freigaben-Modus ist eine ideale Lösung.

Eine andere Situation, die Einfachheit garantiert, ist ein Büro, das viele Drucker hat, die von einem einzelnen zentralen Server angesteuert werden. Jeder muss Druckaufträge an die Drucker schicken können, es gibt keinen Grund, irgendwelche Zugriffskontrolle einzusetzen, und vom Druckserver werden keine Dateien bereitgestellt. Wieder ist ein Stand-alone-Server im Freigaben-Modus (share) eine großartige Lösung.

8.2 Hintergrund

Der Begriff *Stand-alone-Server* bedeutet, dass er lokale Authentifikation und Zugriffskontrolle für alle Ressourcen bietet, die über ihn zugänglich sind. Allgemein bedeutet das, dass es eine lokale Benutzer-Datenbank geben wird. Technischer ausgedrückt bedeutet es, dass Ressourcen auf der Maschine entweder im SHARE- oder im USER-Modus verfügbar gemacht werden.

Es ist nichts weiter nötig als das Anlegen von Benutzerkonten. Stand-alone-Server bieten keine Netzwerk-Anmelde-Dienste an. Das bedeutet, dass Maschinen, die diesen Server

benutzen, keine Domänen-Anmeldung auf ihm durchführen. Welchem Anmeldedienst diese Workstations unterstellt sind, ist unabhängig von dieser Maschine. Es ist aber notwendig, jeden Netzwerk-Benutzer dahingehend „*unterzubringen*“, dass der zur Anmeldung benutzte Name lokal auf dem Samba-Stand-alone-Server in einen lokal bekannten Benutzernamen übersetzt (gemappt) wird. Es gibt verschiedene Arten, wie dies geschehen kann.

Samba neigt dazu, die Unterscheidung etwas zu verwischen, was den Begriff des Stand-alone-Servers angeht. Dies rührt daher, dass die Authentifikationsdatenbank lokal oder auf einem Netzwerk-Server liegen kann, sogar wenn der Samba-Server aus der SMB-Protokoll-Perspektive kein Mitglied des Domänen-Sicherheitskontexts ist.

Durch die Verwendung von Pluggable Authentication Modules (PAM) und dem Namens-Service-Switcher (NSSWITCH, der die UNIX-Benutzer-Datenbank verwaltet) kann die Wurzel der Authentifikation auf einem anderen Server liegen. Wir würden dies den Authentifikationsserver nennen. Das bedeutet, dass der Samba-Server die lokale UNIX/Linux-Passwort-DB verwenden kann (`/etc/passwd` oder `/etc/shadow`), die lokale Datei smbpasswd oder ein LDAP-Backend oder sogar via PAM und Winbind einen anderen CIFS/SMB-Server.

8.3 Beispiel-Konfiguration

Die Beispiele, Beispiel 8.3.1 und Abschnitt 8.3.2, wurden entworfen, um Sie zur Einfachheit zu inspirieren. Es ist oft gar zu leicht, einen hohen Grad an Kreativität anzustreben und damit zu viel Komplexität ins Design von Server und Netzwerk zu bringen.

8.3.1 Referenz-Dokumentationsserver

Die Konfiguration eines Read-only-Datenservers, auf den jeder zugreifen kann, ist sehr einfach. Beispiel 8.3.1 ist die `smb.conf`-Datei, die dies tut. Nehmen wir an, dass all die Referenz-Dokumente im Verzeichnis `/export` gespeichert werden und dass die Dokumente einem anderen User als nobody gehören. Keine home-Verzeichnisse werden freigegeben, und es gibt keine Benutzer in der `/etc/passwd`-UNIX-System-Datenbank. Dies ist ein einfach zu administrierendes System.

Im obigen Beispiel Beispiel 8.3.1 ist der Hostname auf GANDALF gesetzt und die Arbeitsgruppe auf den Namen der lokalen Arbeitsgruppe (MITTELERDE), so dass die Maschine gemeinsam mit Maschinen erscheint, die den Benutzern vertraut sind. Das einzige Passwort-Backend, das benötigt wird, ist das „*guest*“-Backend, um die Verwendung von standardmäßigen unprivilegierten Benutzernamen zu erlauben. Da es einen WINS-Server im Netz gibt, machen wir natürlich Gebrauch davon.

8.3.2 Zentrales Druck-Serving

Die Konfiguration eines einfachen Druckservers ist einfach, wenn Sie die richtigen Tools auf Ihrem System haben.

Annahmen:

1. Der Druck-Server darf keine Administration erfordern.

Beispiel 8.3.1. smb.conf für den Referenz-Dokumentationsserver

```
# Globale Parameter

[global]
        workgroup = MITTELERDE
        netbios name = GANDALF
        security = SHARE
        passdb backend = guest
        wins server = 192.168.1.1

[data]
        comment = Data
        path = /export
        guest only = Yes
```

2. Das Druck-Spooling- und Verarbeitungssystem auf unserem Druck-Server wird CUPS sein. (Siehe Kapitel **??** „Unterstützung des CUPS-Drucksystems“, für mehr Informationen).

3. Der Druck-Server wird nur Netzwerk-Drucker bedienen. Der Netzwerk-Administrator wird die CUPS-Umgebung korrekt für die Unterstützung der Drucker konfigurieren.

4. Alle Workstations werden nur Postscript-Treiber verwenden. Der gewählte Druckertreiber ist der mit MS Windows mitgelieferte Treiber für den Apple Color LaserWriter.

In diesem Beispiel wird unser Druck-Server alle hereinkommenden Druckaufträge in der Datei `/var/spool/samba` spoolen, bis der Job von Samba an den CUPS-Druck-Prozessor weitergegeben werden kann. Da alle hereinkommenden Verbindungen unter dem anonymen (Gast-)Benutzer laufen werden, sind zwei Dinge erforderlich:

Anonymes Drucken aktivieren

- Das UNIX/Linux-System muss ein **guest**-Konto haben. Der Standard hierfür ist üblicherweise das Konto **nobody**. Um den korrekten Namen zu finden, der für Ihr System zu verwenden ist, führen Sie Folgendes aus:

  ```
  $ testparm -s -v | grep "guest account"
  ```

  Stellen Sie sicher, dass dieses Konto in Ihrer System-Passwort-Datenbank existiert (`/etc/passwd`).

- Das Verzeichnis, in das Samba die Datei spoolen wird, muss Schreibrechte für das Gast-Konto aufweisen. Die folgenden Befehle stellen sicher, dass dieses Verzeichnis benutzbar wird:

  ```
  root# mkdir /var/spool/samba
  root# chown nobody.nobody /var/spool/samba
  ```

```
root# chmod a+rwt /var/spool/samba
```

Der Inhalt von `smb.conf` wird in Beispiel 8.3.2 gezeigt.

Beispiel 8.3.2. smb.conf für das Drucken über den Gast-Zugang

```
# Globale Parameter

[global]
        workgroup = MITTELERDE
        netbios name = GANDALF
        security = SHARE
        passdb backend = guest
        printing = cups
        printcap name = cups

[printers]
        comment = All Printers
        path = /var/spool/samba
        printer admin = root
        guest ok = Yes
        printable = Yes
        use client driver = Yes
        browseable = No
```

ANMERKUNG

Auf CUPS-Systemen gibt es eine Funktionalität, um „*raw*"-Daten direkt an den Drucker weiterzugeben, ohne sie zwischenzeitlich durch CUPS-Druck-Filter zu verarbeiten. Wo die Verwendung dieses Modus gewünscht ist, ist es notwendig, ein raw-Druck-Device zu konfigurieren. Es ist außerdem notwendig, den raw mime-Handler in den Dateien `/etc/mime.conv` und `/etc/mime.types` zu aktivieren. Lesen Sie dazu auch Abschnitt **??**.

8.4 Gängige Fehler

Der größte Fehler ist meist, die Netzwerk-Konfiguration zu komplex zu gestalten. Es bewährt sich, die einfachste Lösung zu wählen, die die momentanen Anforderungen erfüllt.

Kapitel 9

ANLEITUNG ZUR MS WINDOWS NETZWERKKONFIGURATION

9.1 Eigenschaften und Vorzüge

Gelegentlich berichten Netzwerk-Administratoren von Schwierigkeiten, Microsoft Windows Clients zur korrekten Zusammenarbeit mit Samba-Servern zu bringen. Es scheint, daß manche Leute einfach die Tatsache nicht akzeptieren können, daß der richtige Weg, MS Windows Netzwerk Clients zu konfigurieren, präzise derselbe ist, als wenn man Microsoft Windows NT4 oder 200x Server einsetzt. Dennoch gibt es den wiederholten Bedarf, detaillierte Anleitungen zur Konfiguration von Windows Clients zu geben.

Ziel dieses Kapitels ist es, die Konfiguration von MS Windows Clients für die meisten kritischen Aspekte einer solchen Konfiguration grafisch darzustellen. Ein erfahrener Netzwerkadministrator wird nicht weiter an Einzelheiten dieses Kapitels interessiert sein.

9.2 Technische Details

Dieses Kapitel beschäftigt sich mit der Konfiguration des TCP/IP Protokolls und auch mit der Netzwerkumgebung für die meisten aktuell verwendeten Plattformen. Diese sind:

- Microsoft Windows XP Professional.
- Windows 2000 Professional.
- Windows Millennium edition (Me).

9.2.1 TCP/IP Konfiguration

Ein Bauherr muss sicherstellen, dass die gesamte Konstruktion auf Basis einer festen Grundlage entsteht. Dasselbe gilt für TCP/IP-basiertes Vernetzen. Grundlegende Probleme mit Netzwerkkonfigurationen plagen alle Benutzer eines Netzwerkes bis zu deren Lösung.

Microsoft Windows Arbeitsstationen und Server können entweder mit fixen IP-Adressen oder per DHCP konfiguriert werden. Die folgenden Beispiele zeigen die Anwendung von DHCP und beschäftigen sich nur am Rande mit jenen Situationen, in denen fixe IP-Settings verwendet werden können.

Es ist möglich, Shortcuts oder gespeicherte Tastatureingaben zu verwenden, um zu einem bestimmten Konfigurationsbildschim zu gelansgen. Wir haben uns entschieden, alle Beispiele dieses Kapitels auf Basis des **Start** Knopfes zu erläutern.

9.2.1.1 MS Windows XP Professional

Es gibt 2 Wege zu einer Windows XP TCP/IP Konfiguration. Wählen Sie Ihre bevorzugte Methode:

Klicken Sie auf **Start** -> **Systemsteuerung** -> **Netzwerkverbindungen**

Alternativ klicken Sie auf **Start** ->, und rechtsklicken Sie **Meine Netzwerkverbindungen**, dann wählen Sie **Eigenschaften**

Der folgende Ablauf durchläuft den Windows XP Professional TCP/IP Konfigurationsprozess:

1. Bei manchen Installationen nennt sich das Interface **Lokale Verbindungen**, bei anderen werden diese **Netzwerkverbindungen** genannt. Auf unserem System heissen Sie **Netzwerkverbindungen**. Rechtsklicken Sie auf **Netzwerkverbindungen** -> **Eigenschaften**. Siehe auch Abbildung 9.1.

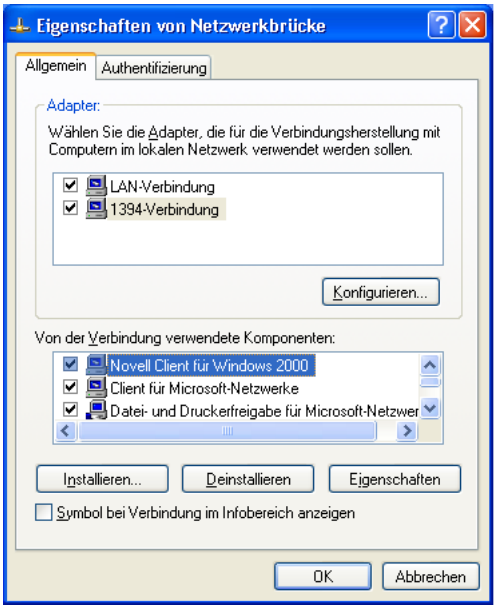


Figure 9.1. Konfiguration Netzwerkverbindungen

2. Das Menü zur Konfiguration der Netzwerkverbindungen oder LAN-Verbindungen wird für die Einstellungen des TCP/IP Protokolles benutzt. In der Box **Diese Verbindung verwendet folgende Elemente:** klicken Sie auf **Internetprotokoll (TCP/IP)** dann auf **Eigenschaften**. Die Standardeinstellung ist aktiviertes DHCP (d.h. „*IP-Adresse automatisch beziehen*“. Siehe auch Abbildung 9.2.

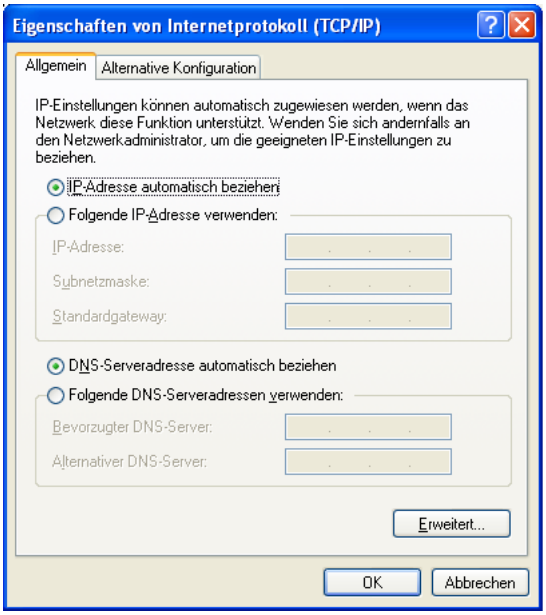


Figure 9.2. Eigenschaften von Internetprotokoll (TCP/IP)

Viele Netzwerkadministratoren nutzen gerne DHCP, um die Client-seitigen TCP/IP-Protokoll-Einstellungen zu setzen. (Für Informationen, wie man einen ISC DHCP-Server mit Microsoft Windows Client-Unterstützung einrichtet, sehen Sie bitte Abschnitt **??**. Falls es erforderlich sein sollte, eine fixe IP-Adresse zur Verfügung zu stellen, klicken Sie auf „*Folgende IP-Adresse verwenden*“ und fahren Sie fort mit der Eingabe der IP-Adresse, der Subnetzmaske und des Standardgateways in der geöffneten Box.

3. Klicken Sie auf den Knopf **Erweitert** um mit der TCP/IP-Konfiguration fortzufahren. Dies öffnet eine Box, in welcher Sie zusätzliche IP-Adressen eingeben können. Die technische Bezeichnung für die zusätzlichen IP-Adressen lautet *IP-Aliase* und in dieser Box kann man weitere Standard-Gateways (oder Router) eingeben. In den meisten Fällen, in denen DHCP genutzt wird, ist es nicht erforderlich, weitere Einstellungen vorzunehmen. Siehe auch Abbildung 9.3, um das Erscheinungsbild dieser Box zu sehen.

   Fixe Einstellungen für DNS und WINS sind vielleicht noch erforderlich, falls diese nicht automatisch durch DHCP zur Verfügung gestellt wurden.

4. Klicken Sie auf die **DNS** Registerkarte, um DNS-Server-Einstellungen hinzuzufügen. Dieses Beispielsystem nutzt manuell gesetzte DNS-Einstellungen. Wenn Sie fertig mit

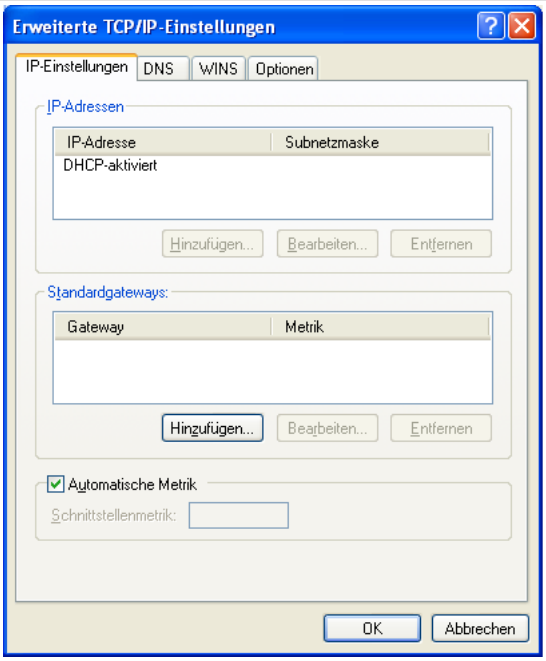


Figure 9.3. Erweiterte TCP/IP Einstellungen

Ihren Änderungen sind, klicken Sie auf den **OK** Knopf, um Ihre Einstellungen zu speichern. Siehe auch Abbildung 9.4.

5. Klicken Sie die **WINS** Registerkarte, um zusätzliche manuelle WINS-Server-Einträge vorzunehmen. Dieser Schritt zeigt ein Beispielsystem, welches manuell gesetzte WINS-Einstellungen nutzt. Wenn Sie fertig mit Ihren Änderungen sind, klicken Sie auf den **OK** Knopf, um Ihre Einstellungen zu speichern. Siehe auch Abbildung 9.5.

9.2.1.2 MS Windows 2000

Es gibt 2 Wege zu einer Windows 2000 Professional TCP/IP Konfiguration. Wählen Sie Ihre bevorzugte Methode:

Klicken Sie auf **Start** -> **Systemsteuerung** -> **Netzwerkverbindungen**

Alternativ klicken Sie auf **Start** ->, und rechtsklicken Sie **Meine Netzwerkverbindungen**, dann wählen Sie **Eigenschaften**

Der folgende Ablauf durchläuft den Windows 2000 Professional TCP/IP Konfigurationsprozess:

1. Rechtsklicken Sie auf **Netzwerkumgebung**, dann klicken Sie auf **Eigenschaften**. Siehe auch Abbildung 9.6.

2. Die Eigenschaften der Netzwerkumgebung werden für die Einstellungen des TCP/IP Protokolls genutzt. Klicken Sie auf **Internetprotokoll (TCP/IP)** in der Box **Aktivierte**

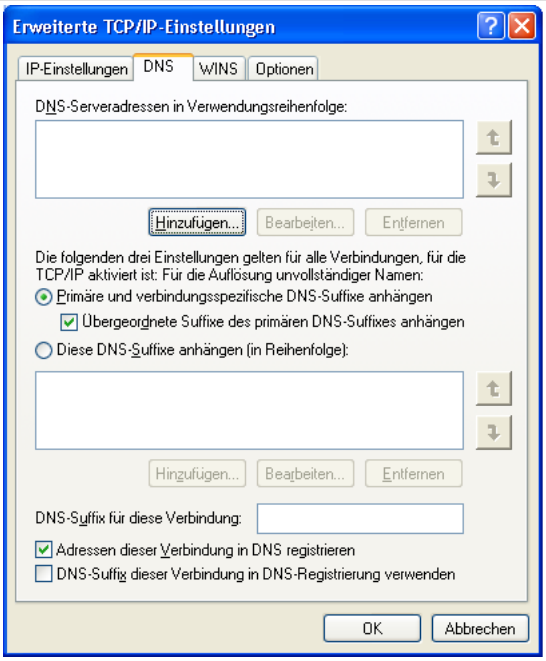


Figure 9.4. DNS Konfiguration

Komponenten werden von dieser Verbindung genutzt: dann klicken Sie auf den **Eigenschaften** Knopf.

3. Die Standardeinstellung ist aktiviertes DHCP (z.B. „*IP-Adresse automatisch beziehen*“. Siehe auch Abbildung 9.7.

   Viele Netzwerkadministratoren nutzen gerne DHCP, um die Client-seitigen TCP/IP-Protokoll-Einstellungen zu setzen. (Für Informationen, wie man einen ISC DHCP-Server mit Microsoft Windows Client-Unterstützung einrichtet sehen Sie bitte Abschnitt **??**. Falls es erforderlich sein sollte, eine fixe IP-Adresse zur Verfügung zu stellen, klicken Sie auf „*Folgende IP-Adresse verwenden*“ und fahren Sie fort mit der Eingabe der IP-Adresse, der Subnetzmaske und des Standardgateways in der geöffneten Box.

4. Klicken Sie auf den Knopf **Erweitert**, um mit der TCP/IP-Konfiguration fort zu fahren. Dies öffnet eine Box, in welcher Sie zusätzliche IP-Adressen eingeben können. Die technische Bezeichnung für die zusätzlichen IP-Adressen lautet *IP-Aliase* und in dieser Box kann man weitere Standard-Gateways (oder Router) eingeben. In den meisten Fällen, in denen DHCP genutzt wird, ist es nicht erforderlich weitere Einstellungen vorzunehmen. Siehe auch Abbildung 9.8 um das Erscheinungsbild dieser Box zu sehen.

   Fixe Einstellungen für DNS und DHCP sind vielleicht noch erforderlich, falls diese nicht automatisch durch DHCP zur Verfügung gestellt wurden.

5. Klicken Sie auf die **DNS** Registerkarte um DNS-Server-Einstellungen hinzuzufügen. Dieses Beispielsystem nutzt manuell gesetzte DNS-Einstellungen. Wenn Sie fertig mit

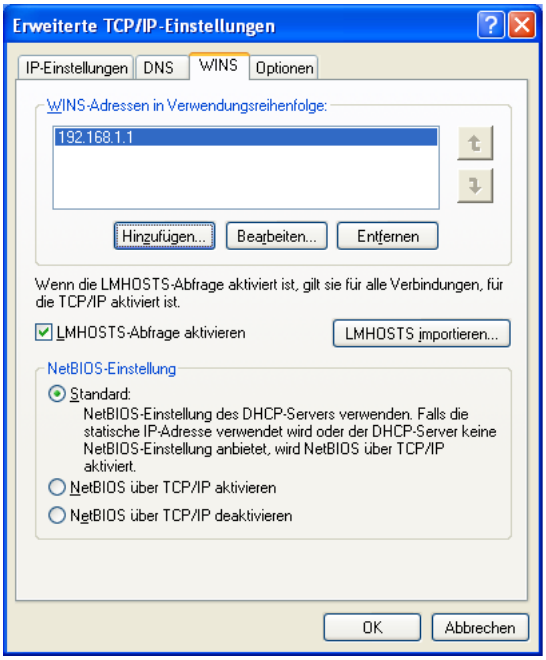


Figure 9.5. WINS Konfiguration

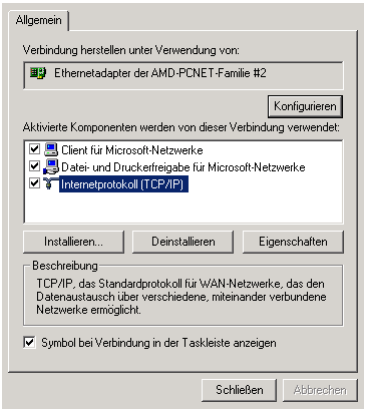


Figure 9.6. Eigenschaften Netzwerkumgebung

Ihren Änderungen sind, klicken Sie auf den Knopf **OK**, um Ihre Einstellungen zu speichern. Siehe auch Abbildung 9.9.

6. Klicken Sie die Registerkarte **WINS**, um zusätzliche manuelle WINS-Server-Einträge vorzunehmen. Dieser Schritt zeigt ein Beispielsystem, welches manuell gesetzte WINS-Einstellungen nutzt. Wenn Sie fertig mit Ihren Änderungen sind, klicken Sie auf den Knopf **OK**, um Ihre Einstellungen zu speichern. Siehe auch Abbildung 9.10.

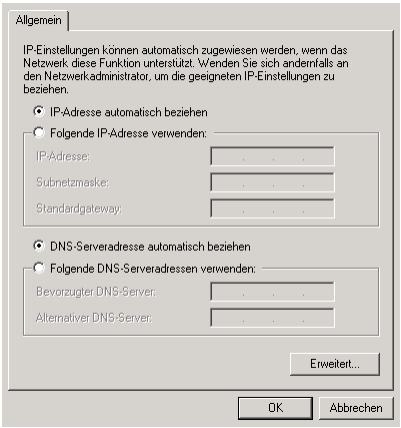


Figure 9.7. Eigenschaften Internetprotokoll (TCP/IP)

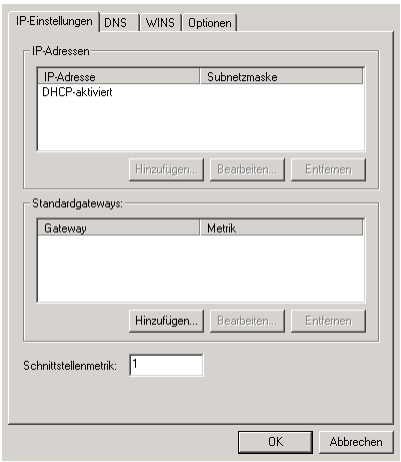


Figure 9.8. Erweiterte TCP/IP Einstellungen

9.2.1.3 MS Windows Me

Es gibt 2 Wege zu einer Windows Millenium Edition (Me) TCP/IP Konfiguration. Wählen Sie Ihre bevorzugte Methode:

Klicken Sie auf **Start** -> **Systemsteuerung** -> **Netzwerk Verbindungen**

Alternativ klicken Sie auf **Start** ->, und rechtsklicken Sie **Meine Netzwerkverbindungen**, dann wählen Sie **Eigenschaften**

Der folgende Ablauf durchläuft den Windows Me TCP/IP Konfigurationsprozess:

1. In der Box **Die folgenden Netzwerkkomponenten sind installiert:** klicken Sie auf den Knopf **Internetprotokoll TCP/IP**, dann auf **Eigenschaften**. Siehe auch Abbildung 9.11.

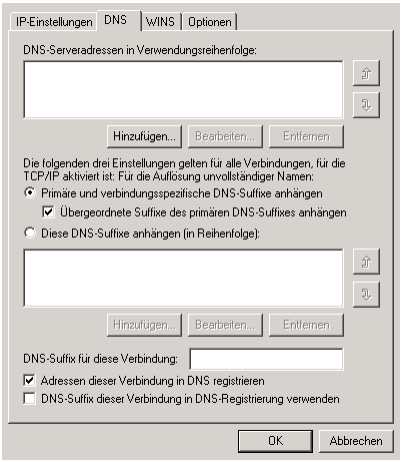


Figure 9.9. DNS Konfiguration

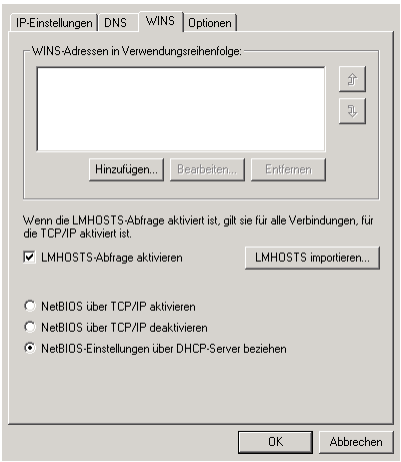


Figure 9.10. WINS Konfiguration

2. Viele Netzwerkadministratoren nutzen gerne DHCP um die Client-seitigen TCP/IP Protokoll-Einstellungen zu setzen. (Für Informationen, wie man einen ISC DHCP-Server mit Microsoft Windows Client-Unterstützung einrichtet sehen Sie bitte Abschnitt **??**. Die Standardeinstellung auf Microsoft Windows Me workstations ist DHCP aktivierte Vorgehensweise, z.B. ist **IP-Adresse automatisch beziehen** aktiviert. Siehe auch Abbildung 9.12.

   Falls es erforderlich sein sollte, eine fixe IP-Adresse zur Verfügung zu stellen, klicken Sie auf „*Folgende IP-Adresse verwenden*“ und fahren Sie fort mit der Eingabe der IP-Adresse, der Subnetzmaske und des Standardgateways in der geöffneten Box. In diesem Beispiel gehen wir davon aus, dass alle Netzwerkclients durch DHCP konfiguriert wurden.

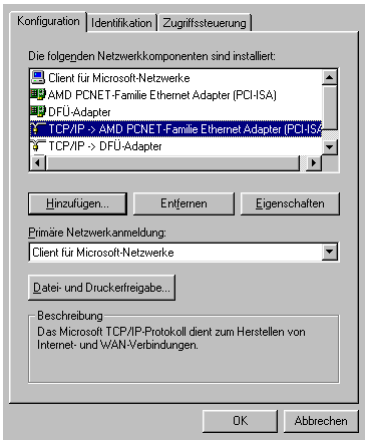


Figure 9.11. Die Windows Me Netzwerkkonfigurations-Box

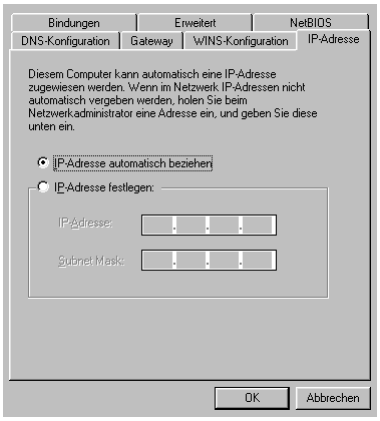


Figure 9.12. IP Addresse

3. Fixe Einstellungen sind vielleicht für DNS und WINS gewünscht, wenn diese Einstellungen nicht per DHCP automatisch zur Verfügung gestellt wurden.

4. Falls notwendig, klicken Sie auf die Registerkarte **DNS Konfiguration**, um einen DNS-Server-Eintrag vorzunehmen. Klicken Sie auf die Registerkarte **WINS Konfiguration**, , um einen WINS-Server-Eintrag vorzunehmen. Die Registerkarte **Gateway** erlaubt es, zusätzliche Gateways (Router-Adressen) in den Netzwerkkarten-Einstellungen zu hinterlegen. In den meisten Fällen, in denen DHCP genutzt wird, wird an dieser Stelle keine manuelle Einstellung notwendig sein.

5. Das folgende Beispiel zeigt manuell konfigurierte WINS Einstellungen. Siehe auch Abbildung 9.13. Wenn die Änderungen fertig sind, klicken Sie **OK**, um diese abzuspeichern.

   Dies ist ein Beispiel dafür, wie ein System manuell konfigurierte WINS-Einstellungen

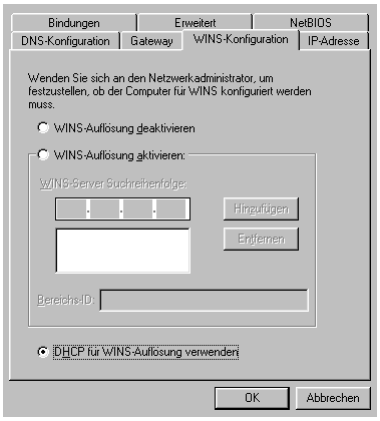


Figure 9.13. DNS Konfiguration

nutzt. Eine Situation, in der dies auftritt, kann ein Netzwerk sein, in dem ein einzelner DHCP-Server Einstellungen für mehrere Windows-Arbeitsgruppen oder -Domänen zur Verfügung stellt. Siehe auch Abbildung 9.14.

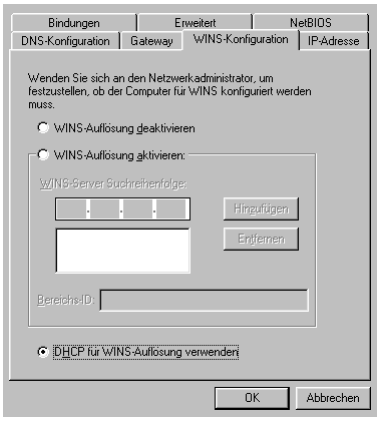


Figure 9.14. WINS Konfiguration

9.2.2 Einer Domäne beitreten: Windows 2000/XP Professional

Microsoft Windows NT/200x/XP Professional Plattformen können an einer Sicherheitsdomäne teilnehmen. Dieser Abschnitt beschreibt den Prozess, der eine Windows 200x/XP Professional Maschine zum Mitglied einer Sicherheitsdomänen-Umgebung macht. Es sollte beachtet werden, dass dieser Prozess beim Beitreten zu einer von Windows NT4/200x kontrollierten Domäne der gleiche wie bei einem Samba PDC ist.

1. Klicken Sie **Start**.

2. Rechtsklicken Sie **Arbeitsplatz**, dann wählen Sie **Eigenschaften**.

3. Die sich öffnende Box ist diesselbe, wie wenn Sie **System** in der Systemsteuerung anwählen. Siehe auch Abbildung 9.15.

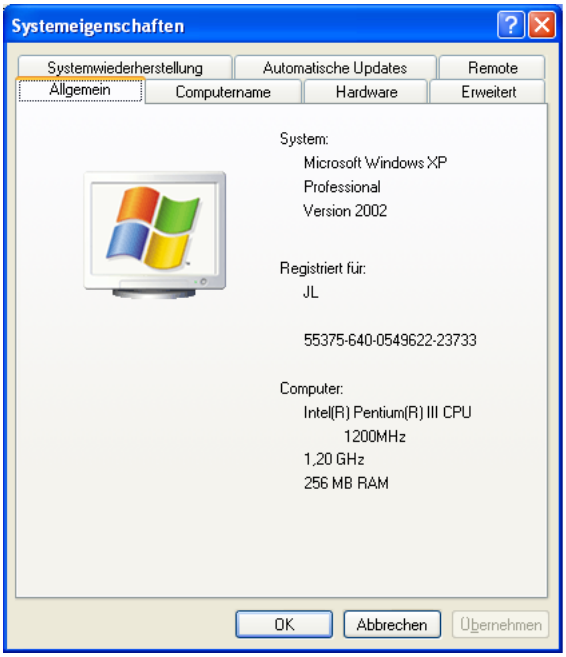


Figure 9.15. Die Hauptbox

4. Klicken Sie auf die Registerkarte **Computername**. Die Box zeigt Ihnen **Computerbeschreibung**, den **Computernamen**, und **Arbeitsgruppe** oder **Domänenname**. Klicken Sie auf den Knopf **Netzwerkkennung**, welcher den Konfigurationswizard startet. Benutzen Sie diesen nicht mit Samba-3. Falls Sie die Änderung des Computernamens oder das Verlassen oder Beitreten der Domäne wünschen, klicken Sie den **Ändern** Knopf. Siehe auch Abbildung 9.16.

5. Klicken Sie auf **Ändern**. Diese Anzeige zeigt, dass unsere Bespielmaschine (TEMPTATION) in einer WORKGROUP genannten Arbeitsgruppe ist. Wir werden der Domäne MITTELERDE beitreten. Siehe auch Abbildung 9.17.

6. Geben Sie den Namen **MITTELERDE** in dem Feld unter dem Domänen-Knopf ein. Diese Box zeigt nun, dass unsere Beispielmaschine (TEMPTATION) ausgewählt ist, um der Domäne MITTELERDE beizutreten. Siehe auch Abbildung 9.18.

7. Jetzt klicken Sie auf **OK**. Eine Dialogbox sollte erscheinen, welche Ihnen die Eingabe der Referenzen (Benutzername und Passwort) eines Domänen-administrativen Accounts ermöglicht, der die Rechte hat, eine Maschine einer Domäne hinzuzufügen. Geben Sie den Namen „*root*“ und das root Passwort Ihres Samba-3 Servers ein. Siehe auch Abbildung 9.19.

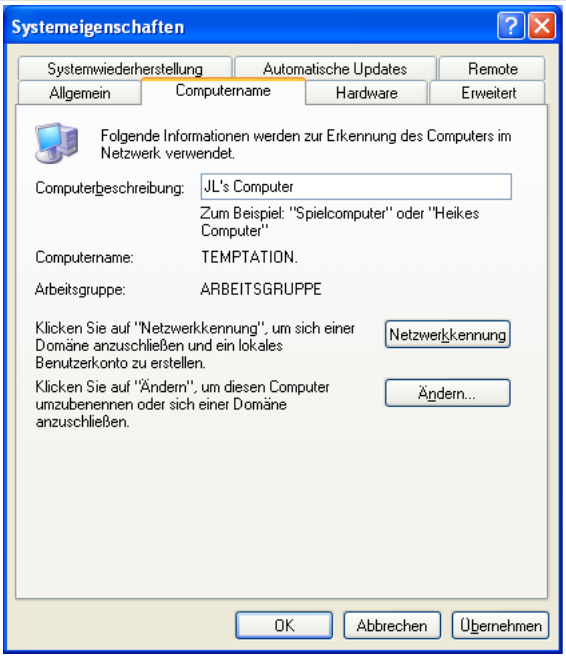


Figure 9.16. Die Box Computername

8. Klicken Sie auf **OK**. Die Dialogbox „*Willkommen in der Domäne MITTELERDE*“ sollte erscheinen. An dieser Stelle muss der Rechner neu gestartet werden. Danach ist das Beitreten zur Domäne abgeschlossen.

9.2.3 Konfiguration der Domänen-Anmeldung: Windows 9x/Me

Wir folgen den Konventionen, die meist besagen, dass Windows 9x/Me Maschinen an Domänen-Anmeldungen teilhaben können. In Wahrheit benutzen diese Plattformen jedoch nur das LanManager Netzwerk-Anmelde-Protokoll.

ANMERKUNG

Windows XP Home Edition kann nicht an Domänen- oder LanManager-Netzwerkanmeldungen teilhaben !

1. Rechtsklicken Sie das Symbol **Netzwerkumgebung**.
2. Das Feld Netzwerk-Konfiguration erlaubt, alle allgemeinen Netzwerk-Einstellungen zu ändern. Siehe auch Abbildung 9.20.

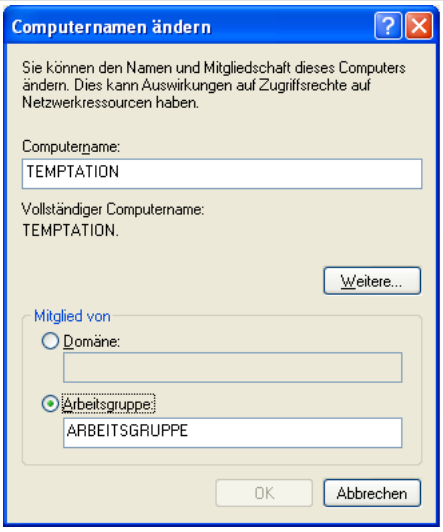


Figure 9.17. Die Box mit der Computernamens-Änderung

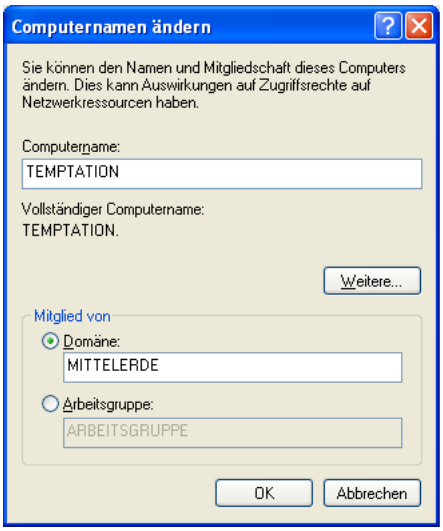


Figure 9.18. Die Box mit der Computernamens-Änderung Domäne MITTELERDE.

Stellen Sie sicher, dass der **Client für Microsoft Netzwerke** wie gezeigt installiert ist. Klicken Sie auf den Eintrag **Client für Microsoft Netzwerke** in **Die folgenden Netzwerkkomponenten sind installiert:**. Dann klicken Sie den Knopf **Eigenschaften**.

3. Die Eigenschaftsseite des Feldes des Client für Microsoft Netzwerke ist die richtige Stelle, um die Einstellungen für die Netzwerkanmeldungen zu konfigurieren. Siehe auch Abbildung 9.21.

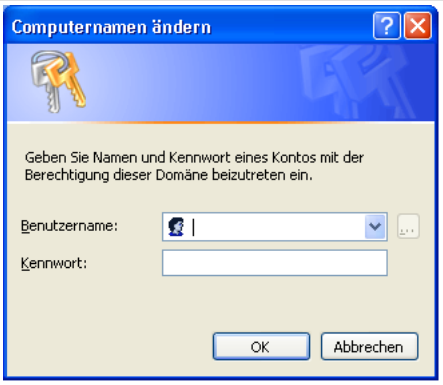


Figure 9.19. Änderung Computername Benutzername und Passwort

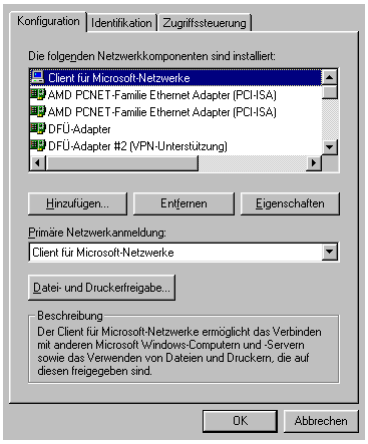


Figure 9.20. Das Feld Netzwerk

Geben Sie den Windows NT Domänennamen ein, überprüfen Sie die Box **Anmelden an einer Windows NT Domäne** und klicken Sie dann **OK**.

4. Klicken Sie den **Erkennen** Knopf. Dies ist die beste Stelle zum Setzen des Arbeitsgruppen- (Domänen-) Namens und des Maschinennamens (Computername). Siehe auch Abbildung 9.22.

5. Jetzt klicken Sie auf den Knopf **Zugriffskontrolle**. Falls Sie in der Lage sein möchten, Freigabe-Zugriffsrechte durch Domänenbenutzer und Gruppenkonten zuzuweisen, dann ist es notwendig, dass Sie wie in dieser Box **Benutzerbasierte Zugriffskontrolle** auswählen. Siehe auch Abbildung 9.23.

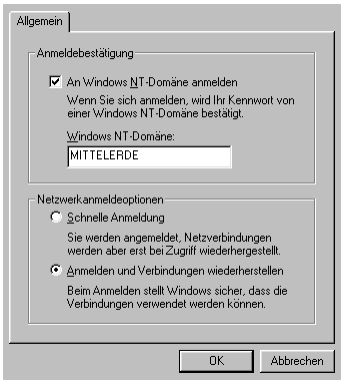


Figure 9.21. Client für Microsoft Netzwerke Eigenschaftsseite

Figure 9.22. Erkennungsbox.

9.3 Allgemeine Fehler

Die häufigsten Fehler, die Windows Netzwerksysteme plagen, beinhalten:

- Faslche IP-Adressen.
- Falsche oder inkonsistente Netzmasken.
- Faslche Routeradressen.
- Falsche DNS Serveradressen.
- Falsche WINS Serveradressen.
- Nutzung von Netzwerk Scope Einstellungen — achten Sie auf diese!

Die häufigsten Gründe, warum ein Windows NT/200x/XP Professional Client eine Sambakontrollierte Domäne nicht erreichen kann, sind:

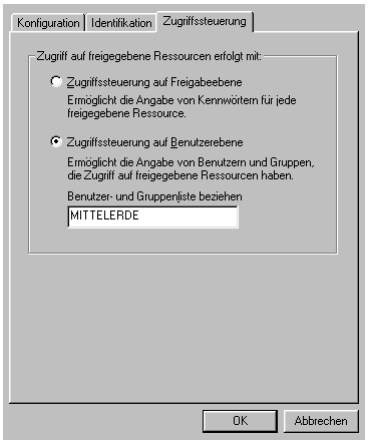


Figure 9.23. Erkennungsbox.

- `smb.conf` hat kein korrektes add machine script.
- Der Account „*root*“ ist nicht in der Passwortdatenbank.
- Der Versuch, einen Benutzeraccount für den Zutritt der Maschine zu einer Domäne zu verwenden, anstatt des „*root*“-Accounts.
- Offene Verbindungen der Arbeitsstation zum Server.
- Firewall- oder Filtereinstellungen entweder auf dem Client oder dem Samba-Server.

Teil III

Erweiterte Konfiguration

WERTVOLLE INFORMATIONEN

Samba hat verschiedene Merkmale die Sie vielleicht nutzen möchten. Dieses Kapitel behandelt ausgewählte Merkmale.

Kapitel 10

NETZWERK-BROWSING

Diese Dokumentation enthält detaillierte Informationen und einen Leitfaden dazu, wie man das Browsing über mehrere Subnetze und/oder Arbeitsgruppen (oder Domänen) hinweg implementiert. WINS ist das beste Werkzeug, um NetBIOS-Namen in IP-Adressen aufzulösen. WINS hat nichts mit Browse-Listen zu tun, außer bei der Auflösung von Namen in Adressen.

ANMERKUNG

MS Windows 2000 und neuere Windows-Versionen können so konfiguriert werden, dass sie ohne NetBIOS über TCP/IP arbeiten, wozu Samba ab Version 3 ebenfalls in der Lage ist. Ist die Benutzung von NetBIOS über TCP/IP deaktiviert, werden die MS Windows-Maschinen über DNS und Active Directory aufgelöst. Die folgenden Informationen gehen davon aus, dass ein Netz mit NetBIOS über TCP/IP betrieben wird.

10.1 Planung und Beginn

Jemand bezog sich einst auf die Vergangenheit mit den Worten „Es war die beste aller Zeiten, es war die schlechteste aller Zeiten.“ Je mehr wir zurückblicken, umso mehr sehnen wir uns nach dem, was war, und hoffen, dass es nie wiederkehrt.

Diese Aussage beschreibt präzise die Gefühle vieler MS Windows Netzwerk-Administratoren in Hinblick auf NetBIOS. Diejenigen, die NetBIOS gemeistert haben, wussten, was sie erwartet. Denjenigen, die es nie geschafft haben, seine Eigenschaften zu zähmen, erscheint NetBIOS wie Pattersons Fluch.

Für diejenigen, die nicht mit den botanischen Problemen Australiens vertraut sind: Pattersons Fluch, *Echium plantagineum*, wurde Mitte des 19. Jahrhunderts eingeführt. Seitdem hat es sich schnell ausgebreitet. Die hohe Samenproduktion der Pflanze mit einer Dichte von Tausenden Samen pro Quadratmeter, ihre Lebensdauer von mehr als sieben Jahren und ihre

Fähigkeit, unter guten Voraussetzungen über das ganze Jahr hinweg zu keimen, sind einige der Eigenschaften, die sie zu einem solch hartnäckigen Unkraut machen. (Frank Patterson war einer der gefürchtetsten Gesetzlosen Australiens. Nachdem er wegen eines Diebstahls von vier Dollar am Galgen landete, verfluchte er die Stadt Ironbark und die australische Regierung. Seine Familie pflanzte eine lilafarbene, aus England stammende Pflanze auf sein Grab, die sich rasch im ganzen Land ausbreitete. Aufgrund der Giftigkeit der Pflanze kostet ihre Vernichtung die Viehzüchter Australiens ca. 30 Mill. Dollar pro Jahr, Anm. d. Übersetzers.)

In diesem Kapitel erfahren wir die grundlegenden Aspekte der Server Message Block-(SMB-)Vernetzung mit einem besonderen Blick auf SMB als Implementation in einer NetBIOS-über-TCP/IP-Umgebung (NetBIOS = Network Basic Input/Output System). Da Samba SMB oder NetBIOS nicht über ein anderes Protokoll implementiert, ist es wichtig zu wissen, wie man die Netzwerkumgebung konfiguriert, und sich schlicht daran zu erinnern, nichts anderes als TCP/IP auf allen MS Windows-Clients im Netzwerk zu benutzen.

Samba bietet die Möglichkeit, WINS (Windows Inter-networking Name Server) samt der Systemerweiterungen von Microsofts WINS zu implementieren. Diese Systemerweiterungen helfen Samba dabei, stabile WINS-Operationen - über den herkömmlichen Anwendungsbereich von MS WINS hinaus - zu ermöglichen.

WINS wirkt sich ausschließlich auf Systeme aus, die mit NetBIOS-über-TCP/IP laufen. MS Windows 200x/XP können NetBIOS abschalten. In so einem Fall spielt WINS keine Rolle mehr. Samba unterstützt dies ebenfalls.

In Netzwerken, in denen NetBIOS deaktiviert ist, d.h. wo WINS nicht mehr benötigt wird, ist der Einsatz eines DNS für die Namensauflösung unabdingbar.

10.2 Was ist Browsing?

Für die meisten bedeutet Browsing, dass sie die MS Windows- und Samba-Server in der Netzwerkumgebung sehen können und dass, wenn man auf das Icon eines bestimmten Servers klickt, ein Fenster geöffnet wird, in dem man die verfügbaren Freigaben und Drucker des Servers sehen kann.

Was so einfach klingt, ist in Wirklichkeit eine komplexe Interaktion verschiedener Technologien. Die dabei involvierten Technologien (oder Methoden) beinhalten Folgendes:

- MS Windows-Maschinen melden ihre Präsenz im Netzwerk an.
- Maschinen kündigen sich anderen Maschinen im Netzwerk an.
- Eine oder mehrere Maschinen fassen diese Ankündigungen lokal zusammen.
- Der Client findet die Maschine, die diese Liste von Maschinen gesammelt hat.
- Der Client ist in der Lage, den Namen der Maschine in eine IP-Adresse aufzulösen.
- Der Client ist in der Lage, sich mit einer anderen Maschine zu verbinden.

Die Samba-Anwendung, die die Verwaltung des Browsings und die Namensauflösung kontrolliert, heißt `nmbd`. Die dabei verwendeten Konfigurationsparameter sind:

Browsing-Optionen: os level(*), lm announce, lm interval, preferred master(*), local master(*), domain master(*), browse list, enhanced browsing.

Namensauflösungsmethoden: name resolve order(*).

WINS-Optionen: dns proxy, wins proxy, wins server(*), wins support(*), wins hook.

Für Samba sind der WINS-Server und die WINS-Unterstützung zwei einander ausschließende Optionen. Die mit (*) markierten Optionen sind die einzigen Optionen, die im Allgemeinen verändert werden müssen. Sogar wenn keiner dieser Parameter gesetzt ist, tut `nmbd` nach wir vor seinen Job.

10.3 Diskussion

Die gesamte MS Windows-Netzwerk-Technologie verwendet „*SMB Messaging*“. Dieses kann mit oder ohne NetBIOS implementiert werden. MS Windows 200x unterstützt NetBIOS-über-TCP/IP, um Rückwärtskompatibilität zu gewährleisten. Microsoft scheint zu planen, die NetBIOS-Unterstützung auslaufen zu lassen.

10.3.1 NetBIOS-über-TCP/IP

Samba implementiert NetBIOS, wie es auch MS Windows NT/200x/XP tut, indem es dieses Protokoll in TCP/IP einbettet. NetBIOS-basierendes Netzwerke verwenden Broadcasts, um die Verwaltung der Browse-Listen zu regeln. Wenn man NetBIOS-über-TCP/IP ausführt, verwendet dieses das UDP-Messaging. Diese UDP-Nachrichten können Broadcasts oder Unicasts sein.

Normalerweise können nur Unicast-UDP-Messages von Routern weitergeleitet werden. Der Parameter remote announce in `smb.conf` hilft dabei, die Ankündigungen und Aktualisierungen der Browse-Listen über Unicast-UDP an entfernte Netzwerksegmente weiterzugeben. In ähnlicher Weise implementiert der Parameter remote browse sync in `smb.conf` die Sammlung und Zusammenfügung von Browse-Listen mit Unicast-UDP.

Außerdem sollte `nmbd` in jenen Netzen, in denen Samba die einzige SMB-Server-Technologie ist, nach Möglichkeit auf einer Maschine als der WINS-Server konfiguriert werden. Das macht es einfach, die Browsing-Umgebung zu verwalten. Wenn jedes Netzwerk-Segment mit seinem eigenen Samba-WINS-Server konfiguriert ist, dann besteht der einzige Weg, das Browsing über mehrere Segmente zu ermöglichen, in der Verwendung der Parameter remote announce und remote browse sync in Ihrer `smb.conf`.

Wenn nur ein WINS-Server für ein gesamtes Multi-Segment-Netzwerk verwendet wird, dann sollte die Verwendung der Parameter remote announce und remote browse sync nicht erforderlich sein.

Seit Samba-3 wird an der Replikation von WINS gearbeitet. Der Großteil des Codes wurde bereits ins Samba-SVN übernommen, muss aber noch „*reifen*“. Diese Replikation ist kein unterstütztes Feature der Samba-3.0.0-Release. Hoffentlich wird es in einer der folgenden Samba-3-Releases zu einem unterstützten Feature.

Derzeit unterstützt das Samba-WINS keine MS-WINS-Replikation. Das bedeutet: Wenn Sie einen Samba-Server als WINS-Server einrichten, darf nur *ein* `nmbd` als WINS-Server im

Netzwerk konfiguriert sein. Manche Installationen haben mehrere Samba-WINS-Server aus Gründen der Redundanz eingesetzt (ein Server pro Subnetz) und dann remote announce und remote browse sync verwendet, um die Sammlung und Zusammenführung der Browse-Listen über alle Segmente zu erzielen. Beachten Sie, dass dies bedeutet, dass Clients nur lokale Namen auflösen, und so konfiguriert werden müssen, dass sie DNS zur Auflösung von Namen anderer Subnetze verwenden, um es ihnen zu ermöglichen, die IP-Adressen der Server anderer Subnetze aufzulösen. Dieses Setup wird nicht empfohlen, wird aber aus Gründen der Vollständigkeit und aus praktischen Überlegungen aufgeführt (d.h. als Szenario für den Moment, „*wenn alles andere schief geht*“).

Zuletzt sollten Sie noch beachten, dass Browse-Listen eine Sammlung von unzuverlässigen Broadcast-Nachrichten sind, die in Intervallen von nicht mehr als 15 Minuten wiederholt werden. Das bedeutet, dass es Zeit braucht, eine Browse-Liste zu bilden, und dass es bis zu 45 Minuten dauern kann, bis diese sich stabilisiert, speziell über verschiedene Netzwerk-Segmente hinweg.

10.3.2 TCP/IP ohne NetBIOS

Alle TCP/IP-fähigen Systeme verwenden verschiedene Formen der Namensauflösung. Die primären Methoden für die TCP/IP-Namensauflösung sehen entweder eine statische Datei (`/etc/hosts`) vor oder DNS (Domain Name System). DNS ist die Technologie, die das Internet benutzbar macht. Die DNS-basierende Namensauflösung wird von fast allen TCP/IP-fähigen Systemen unterstützt, nur ein paar wenige „*embedded*“ TCP/IP-Systeme unterstützen kein DNS.

Wenn ein MS Windows 200x/XP-System versucht, einen Hostnamen zu einer IP-Adresse aufzulösen, folgt es einem definierten Pfad:

1. Prüfung der Datei `hosts`. Diese befindet sich in `C:\Windows NT\System32\Drivers\etc`.
2. Ausführung einer DNS-Abfrage
3. Prüfung des NetBIOS-Namens-Cache
4. Abfrage des WINS-Servers
5. Ausführung einer Broadcast-Abfrage über UDP
6. Überprüfung der Datei LMHOSTS, in `C:\Windows NT\System32\Drivers\etc`

Windows 200x/XP kann seinen Hostnamen an einem „*Dynamic DNS Server*“ registrieren. Sie können dies erzwingen: **ipconfig /registerdns**.

Wenn Sie Active Directory (ADS) verwenden, brauchen Sie unbedingt einen korrekt funktionierenden DNS-Server. Fehlt ein korrekt funktionierender und arbeitender DNS-Server, sind die MS Windows-Clients und Server nicht mehr imstande, einander gegenseitig zu finden. Daher werden in der Folge auch die Netzwerkdienste ernsthaft geschädigt.

Die Verwendung von „*Dynamic DNS*“ mit Active Directory wirdwärmstens empfohlen, wobei auch der Einsatz von BIND9 vorzuziehen ist (wegen seiner Fähigkeit zur adäquaten Unterstützung der SRV-Einträge, die für Active Directory benötigt werden).

10.3.3 DNS und Active Directory

Gelegentlich hören wir von UNIX-Netzwerk-Administratoren, die einen UNIX-basierenden Dynamic-DNS-Server anstatt des MS-DNS-Servers einsetzen wollen. Dies mag zwar für manche wünschenswert sein, aber der MS Windows 200x-DNS-Server ist für die Zusammenarbeit mit Active Directory automatisch vorkonfiguriert. Es ist möglich, BIND in der Version 8 oder 9 einzusetzen, aber es wird fast mit Sicherheit notwendig sein, SRV-Einträge anzulegen, damit MS Active-Directory-Clients Hostnamen auflösen können, um essenzielle Netzwerkdienste lokalisieren können. Im Folgenden sehen Sie einige der Standard-SRV-Einträge, die Active Directory benötigt:

_ldap._tcp.pdc._msdcs.*Domain* Gibt die Adresse des Windows NT-PDC für die Domäne an.

_ldap._tcp.pdc._msdcs.*DomainTree* Löst die Adressen der „*Global Catalog Server*“ in der Domäne auf.

_ldap._tcp.*site*.sites.writable._msdcs.*Domain* Gibt eine Liste der Domänen-Controller an, die auf den Sites basiert.

_ldap._tcp.writable._msdcs.*Domain* Listet Domänen-Controller auf, die eine schreibberechtigte Kopie des Active Directory führen.

_ldap._tcp.*GUID*.domains._msdcs.*DomainTree* Eintrag, der von MS Windows-Clients verwendet wird, um Maschinen mit dem „*Global Unique Identifier*“ zu lokalisieren.

_ldap._tcp.*Site*.gc._msdcs.*DomainTree* Wird von MS Windows-Clients verwendet, um den „*Global Catalog Server*“ zu lokalisieren, der von der Site-Konfiguration abhängig ist.

Spezifische Einträge, die von MS Windows-Clients verwendet werden, um essenzielle Dienste für eine Beispiel-Domäne namens `quenya.org` zu lokalisieren. Sie beinhalten:

- _kerberos._udp.quenya.org — Wird verwendet, um den KDC-Server über UDP zu kontaktieren. Dieser Eintrag muss für jeden KDC den Port 88 auflisten.
- _kpasswd._udp.quenya.org — Wird verwendet, um den `kpasswd`-Server zu lokalisieren, wenn die Änderung eines Benutzerpassworts bearbeitet werden soll. Dieser Eintrag muss den Port 464 auf dem Master-KDC auflisten.
- _kerberos._tcp.quenya.org — Wird verwendet, um den KDC-Server via TCP zu lokalisieren. Dieser Eintrag muss für jeden KDC den Port 88 auflisten.
- _ldap._tcp.quenya.org — Wird verwendet, um den LDAP-Dienst auf dem PDC zu lokalisieren. Dieser Eintrag muss den Port 389 des PDCs enthalten.
- _kpasswd._tcp.quenya.org — Wird verwendet, um den `kpasswd`-Server zu lokalisieren, um Änderungen von Benutzerpasswörtern zu erlauben. Dieser Eintrag muss den Port

464 enthalten.

- _gc._tcp.quenya.org — Wird verwendet, um den „*Global Catalog Server*“ für die Domäne zu lokalisieren. Dieser Eintrag muss den Port 3268 auflisten.

Die folgenden Einträge werden auch vom Windows Domain-Member-Client verwendet, um wichtige Dienste auf den Windows ADS-Domänencontrollern zu finden.

- _ldap._tcp.pdc._msdcs.quenya.org
- _ldap.gc._msdcs.quenya.org
- _ldap.default-first-site-name._sites.gc._msdcs.quenya.org
- _ldap.{SecID}.domains._msdcs.quenya.org
- _ldap._tcp.dc._msdcs.quenya.org
- _kerberos._tcp.dc._msdcs.quenya.org
- _ldap.default-first-site-name._sites.dc._msdcs.quenya.org
- _kerberos.default-first-site-name._sites.dc._msdcs.queyna.org
- SecID._msdcs.quenya.org

Das Vorhandensein der korrekten DNS-Einträge kann so validiert werden:

```
root#  dig @frodo -t any _ldap._tcp.dc._msdcs.quenya.org

; <lt;>> DiG 9.2.2 <lt;>> @frodo -t any _ldap._tcp.dc._msdcs.quenya.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3072
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2


;; QUESTION SECTION:
;_ldap._tcp.dc._msdcs.quenya.org. IN        ANY


;; ANSWER SECTION:
_ldap._tcp.dc._msdcs.quenya.org. 600 IN SRV 0 100 389 frodo.quenya.org.
_ldap._tcp.dc._msdcs.quenya.org. 600 IN SRV 0 100 389 noldor.quenya.org.


;; ADDITIONAL SECTION:
frodo.quenya.org. 3600  IN      A       10.1.1.16
noldor.quenya.org. 1200  IN      A       10.1.1.17


;; Query time: 0 msec
;; SERVER: frodo#53(10.1.1.16)
```

```
;; WHEN: Wed Oct  7 14:39:31 2004
;; MSG SIZE  rcvd: 171
```

10.4 Wie Browsing funktioniert

MS Windows-Maschinen registrieren ihre NetBIOS-Namen (d.h. den Maschinen-Namen für jeden laufenden Dienst) beim Start. Die genaue Methode, mit der diese Registrierung stattfindet, ist davon abhängig, ob der MS Windows-Client/Server eine WINS-Server-Adresse erhalten hat oder nicht, ob die LMHOSTS-Abfrage aktiviert ist, ob DNS für die Auflösung von NetBIOS-Namen aktiviert ist etc.

Falls es keinen WINS-Server gibt, werden alle Namensregistrierungen wie auch Namensabfragen mit UDP-Broadcasts durchgeführt. Dies beschränkt die Namensauflösung auf das lokale Subnetz, es sei denn, LMHOSTS wird zur Listung aller Namen und IP-Adressen verwendet. In solchen Situationen bietet Samba eine Möglichkeit, mit der der Samba-Server zwangsweise in die Browse-Liste eines fernen MS Windows-Netzwerks eingetragen werden kann (durch den Parameter remote announce).

Wo ein WINS-Server eingesetzt wird, wird der MS Windows-Client einen UDP-Unicast verwenden, um sich am WINS-Server zu registrieren. Solche Pakete können geroutet werden, und daher erlaubt WINS die Namensauflösung über geroutete Netzwerke.

Während des Startvorgangs wird eine Wahl stattfinden, um einen „*Local Master Browser*“ zu bestimmen, wenn nicht bereits ein solcher existiert. In jedem NetBIOS-Netzwerk wird eine Maschine ausgewählt, um als der „*Domain Master Browser*“ zu fungieren. Dieses Domänen-Browsing hat nichts mit dem MS Domänen-Controlling zu tun. Stattdessen übernimmt der Domain Master Browser die Rolle, jeden LMB („*Local Master Browser*“) zu kontaktieren (er wird entweder über WINS oder LMHOSTS ausfindig gemacht), und die Browse-Listen auszutauschen. Auf diese Weise erhält jeder Master Browser eine komplette Liste aller Maschinen im Netzwerk. Alle 11 bis 15 Minuten wird eine Wahl abgehalten, um zu bestimmen, welche Maschine der Master Browser sein soll. Nach den Kriterien dieser Wahl wird die Maschine mit der größten Uptime, der höchsten Protokoll-Version oder anderen Kriterien die Wahl zum „*Domain Master Browser*“ gewinnen.

Clients, die das Netzwerk durchsuchen wollen, verwenden diese Liste, aber sind auch abhängig von der korrekten Namensauflösung in die entsprechenden IP-Adresse(n).

Jede Konfiguration, die die Namensauflösung und/oder die Browsing-Funktionalitäten verletzt, wird die Benutzer verärgern, da sie dann immer wieder damit konfrontiert sind, die Netzwerkdienste nicht verwenden zu können.

Samba unterstützt ein Feature, das die erzwungene Synchronisation von Browse-Listen über geroutete Netzwerke mit dem Parameter remote browse sync in der Datei `smb.conf` erlaubt. Dies veranlasst Samba, den LMB in einem fernen Netzwerk zu kontaktieren und dort die Synchronisation der Browse-Listen zu erfragen. Dies überbrückt effektiv zwei durch Router getrennte Netzwerke. Die beiden entfernten Netzwerke können entweder eine broadcast-basierende oder eine WINS-basierende Namensauflösung verwenden, aber Sie sollten beachten, dass der Parameter remote browse sync die Browse-Listen-Synchronisation anbietet, und diese ist etwas anderes als Namensauflösung. Mit anderen Worten: um das

„*Cross-Subnetz-Browsing*“ korrekt arbeiten zu lassen, ist es unbedingt notwendig, dass ein Mechanismus zur Auflösung von Namen in Adressen vorhanden ist. Dieser Mechanismus kann via DNS, `/etc/hosts` usw. funktionieren.

10.4.1 Konfiguration des ARBEITSGRUPPEN-Browsings

Um das „*Cross-Subnetz-Browsing*“ in einem Netzwerk zu konfigurieren, das Maschinen in einer ARBEITSGRUPPE enthält, nicht solche einer NT Domäne, müssen Sie einen Samba-Server als Domain Master Browser (DMB) einrichten (beachten Sie, dass dies nicht dasselbe wie ein primärer Domänencontroller ist, obwohl in einer NT-Domäne dieselbe Maschine beide Funktionen übernimmt). Die Aufgabe eines Domain Master Browsers ist es, die Browse-Listen von den lokalen Master-Browsern all der Subnetze zu sammeln und zusammenzufügen, die eine Maschine beinhalten, die Teil der Arbeitsgruppe ist. Wäre keine Maschine als Domain Master Browser konfiguriert, würde jedes Subnetz eine isolierte Arbeitsgruppe sein, die unfähig wäre, irgendwelche Maschinen in einem anderen Subnetz zu sehen. Es ist das Vorhandensein eines Domain Master Browsers, das das Cross-Subnetz-Browsing für eine Arbeitsgruppe ermöglicht.

In einer ARBEITSGRUPPEN-Umgebung muss der Domain Master Browser ein Samba-Server sein, und es darf nur einen DMB pro Arbeitsgruppen-Name geben. Um einen Samba-Server als DMB einzurichten, setzen Sie folgende Option im Abschnitt *[global]* der Datei `smb.conf`:

```
domain master = yes
```

Der Domain Master Browser sollte vorzugsweise auch der lokale Master-Browser für sein eigenes Subnetz sein. Um dies zu erreichen, setzen Sie die Optionen im Abschnitt *[global]* der Datei `smb.conf` wie im folgenden Beispiel:

Beispiel 10.4.1. smb.conf für einen Domain Master Browser

```
[global]
        domain master = yes
        local master = yes
        preferred master = yes
        os level = 65
```

Der Domain Master Browser kann dieselbe Maschine wie der WINS-Server sein, sollte es erforderlich sein.

Als Nächstes sollten Sie sicherstellen, dass jedes der Subnetze eine Maschine enthält, die als der lokale Master- Browser für die Arbeitsgruppe arbeiten kann. Jede MS Windows NT/200x/XP-Maschine sollte imstande sein, dies zu tun, genauso wie Windows 9x/Me-Maschinen (obwohl diese dazu neigen, öfter Neustarts zu brauchen; also ist es keine allzu gute Idee, diese dafür zu verwenden). Um einen Samba-Server zu einem lokalen Master-Browser zu machen, setzen Sie die Optionen im Abschnitt *[global]* der Datei `smb.conf` wie im folgenden Beispiel:

Beispiel 10.4.2. smb.conf für einen lokalen Master-Browser

```
[global]
        domain master = no
        local master = yes
        preferred master = yes
        os level = 65
```

Machen Sie das nicht für mehr als einen Samba-Server pro Subnetz, oder diese Rechner werden gegeneinander darum kämpfen, wer denn der lokale Master-Browser sein soll.

Der Parameter local master erlaubt es Samba, als lokaler Master- Browser zu arbeiten. Der Parameter preferred master veranlasst **nmbd** dazu, bei seinem Start eine Browser-Wahl zu erzwingen, und os level stuft Samba so hoch ein, dass es jede Wahl gewinnen sollte.

Wenn Sie eine NT-Maschine im Subnetz haben, die Sie zum lokalen Master-Browser machen wollen, können Sie es Samba „*verbieten*“, ein lokaler Master-Browser zu werden, indem Sie folgende Optionen im Abschnitt *[global]* der Datei `smb.conf` wie im folgenden Beispiel setzen:

Beispiel 10.4.3. smb.conf für einen Samba-Server, der kein Master-Browser ist

```
[global]
        domain master = no
        local master = no
        preferred master = no
        os level = 0
```

10.4.2 Konfiguration des DOMÄNEN-Browsings

Wenn Sie Samba-Server einer Windows-NT-Domäne hinzufügen, dann dürfen Sie keinen Samba-Server als Domain Master Browser einrichten. Standardmäßig ist der Windows NT-PDC einer Domäne auch gleichzeitig der Domain Master Browser für diese Domäne. Das Netzwerk-Browsing kann zusammenbrechen, wenn sich ein Samba-Server mit dem NetBIOS-Namen des Domain Master Browsers zusätzlich zum PDC am WINS-Server anmeldet (*DOMÄNE*<1B>).

Für andere Subnetze als jenes, das den Windows NT PDC enthält, können Sie wie beschrieben Samba-Server als lokale Master-Browser einrichten. Um einen Samba-Server zu einem lokalen Master-Browser zu machen, setzen Sie folgende Optionen im Abschnitt *[global]* der Datei `smb.conf` wie im folgenden Beispiel:

Wenn Sie wollen, dass ein Samba-Server mit anderen Maschinen im Subnetz um den Sieg in der Browsing-Wahl kämpft, können Sie den Parameter os level auf niedrigere Werte setzen. Damit können Sie die Reihenfolge feintunen, in der die Maschinen zum lokalen Master-Browser werden, wenn sie laufen. Mehr Details dazu finden Sie im Abschnitt Wie man Samba dazu zwingt, der Master zu sein.

Beispiel 10.4.4. smb.conf für einen lokalen Master-Browser

```
[global]
        domain master = no
        local master = yes
        preferred master = yes
        os level = 65
```

Wenn Sie Windows NT-Maschinen haben, die Domänenmitglieder auf allen Subnetzen sind, und Sie sich sicher sind, dass diese Maschinen immer laufen werden, können Sie Samba von der Teilnahme an Browsing-Wahlen ausnehmen. Auf diese Weise deaktivieren Sie, dass Samba jemals ein lokaler Master-Browser wird, indem Sie folgende Optionen im Abschnitt *[global]* der Datei `smb.conf` wie im folgenden Beispiel setzen:

Beispiel 10.4.5. smb.conf für einen Samba-Server, der nie Master-Browser wird

```
[global]
        domain master = no
        local master = no
        preferred master = no
        os level = 0
```

10.4.3 Wie man Samba dazu zwingt, der Master zu sein

Wer der Master-Browser wird, hängt von einem Wahlvorgang ab, der Broadcasts verwendet. Jedes Wahl-Paket enthält eine Anzahl von Parametern, die bestimmen, welchen Rang ein Host bei der Wahl einnimmt. Standardmäßig verwendet Samba einen niedrigen Rang und verliert daher die Wahlen gegen so gut wie jeden Windows-Netzwerk-Client oder -Server.

Wenn Sie wollen, dass Samba Wahlen gewinnt, setzen Sie die globale Option os level in `smb.conf` auf einen höheren Wert. Der Standard ist 20. Die Verwendung von 34 ließe Samba alle Wahlen gegen jedes andere System gewinnen (außer gegen andere Samba-Systeme).

Ein os level von 2 würde Samba Windows for Workgroups und Windows 9x/Me schlagen lassen, aber nicht MS Windows NT/200x-Server. Ein MS Windows NT/200x-Server-Domänencontroller verwendet level 32. Das Maximum für os level ist 255.

Wenn Sie wollen, dass Samba bei seinem Start eine Wahl erzwingt, setzen Sie die globale Option preferred master in `smb.conf` auf `yes`. Samba hat dann einen leichten Vorteil gegenüber anderen potenziellen Master-Browsern, die keine „*Preferred Master Browser*“ sind. Verwenden Sie diesen Parameter vorsichtig, denn wenn Sie zwei Hosts (egal ob diese Windows 9x/Me oder NT/200x/XP oder Samba ausführen) im selben Subnetz haben, bei denen preferred master auf `yes` gesetzt ist, werden diese beiden periodisch und kontinuierlich eine Wahl erzwingen, um lokaler Master-Browser zu werden.

Wenn Sie wollen, dass Samba ein *Domain Master Browser* wird, dann ist es zu empfehlen, dass Sie auch preferred master auf `yes` setzen, da Samba nicht zum Domain Master Browser

für Ihr gesamtes LAN oder WAN wird, wenn es nicht auch ein lokaler Master-Browser in seinem eigenen broadcast-isolierten Subnetz ist.

Es ist möglich, zwei Samba-Server so zu konfigurieren, dass sie versuchen, Domain Master Browser für eine Domäne zu werden. Der erste Server, der startet, wird der Domain Master Browser. Alle anderen Samba-Server werden alle fünf Minuten versuchen, zum Domain Master Browser zu werden. Sie werden herausfinden, dass ein anderer Samba-Server bereits der Domain Master Browser ist, und scheitern. Dies gewährt automatisch Redundanz, wenn der aktuelle Domain Master Browser ausfallen sollte.

10.4.4 Wie man Samba zum Domänen-Master macht

Der Domänen-Master ist für die Sammlung und Zusammenführung der Browse-Listen von mehreren Subnetzen verantwortlich, so dass ein Browsing über Subnetze hinweg stattfinden kann. Sie können Samba zum Domänen-Master machen, indem Sie in der Datei `smb.conf` den Parameter domain master = yes setzen. In der Voreinstellung ist Samba kein Domänen-Master.

Machen Sie Samba nicht zum Domänen-Master für eine Arbeitsgruppe, die denselben Namen wie eine NT/200x-Domäne hat. Wenn Samba als Domänen-Master für eine Arbeitsgruppe konfiguriert ist, die sich im selben Subnetz wie eine gleichnamige Windows NT/200x-Domäne befindet, werden mit Sicherheit Browsing-Probleme auftreten.

Wenn Samba Domänen-Master und Master-Browser ist, wird es auf Master-Verlautbarungen (die ca. alle 12 Minuten stattfinden) von lokalen Master-Browsern in anderen Subnetzen hören und diese dann kontaktieren, um die Browse-Listen zu synchronisieren.

Wenn Sie wollen, dass Samba der Domänen-Master ist, sollten Sie auch den Wert für os level ausreichend hoch setzen, um sicherzustellen, dass Samba Browsing-Wahlen gewinnt, und preferred master auf `yes` setzen, um beim Start von Samba eine solche Wahl zu erzwingen.

Alle Server (inklusive Samba) und Clients sollten einen WINS-Server zur NetBIOS-Namensauflösung verwenden. Wenn Ihre Clients nur Broadcasting zur NetBIOS-Namensauflösung verwenden, werden zwei Dinge geschehen:

1. Die lokalen Master-Browser werden nicht mehr imstande sein, einen Domain Master Browser zu finden, da sie nur noch im lokalen Subnetz suchen können.
2. Wenn ein Client doch eine domänen-weite Browse-Liste erhascht und ein Benutzer versucht, auf einen Host in dieser Liste zuzugreifen, wird er nicht imstande sein, den NetBIOS-Namen dieses Hosts aufzulösen.

Wenn jedoch sowohl Samba als auch Ihre Clients einen WINS-Server verwenden, dann gilt Folgendes:

1. Lokale Master-Browser kontaktieren den WINS-Server, und - sofern Samba sich als Domain Master Browser am WINS-Server registriert hat - der lokale Master-Browser empfängt die IP-Adresse des Samba-Servers als die seines Domain Master Browsers.
2. Wenn ein Client eine domänen-weite Browse-Liste erhält und ein Benutzer versucht, auf einen Host in dieser Liste zuzugreifen, kontaktiert der Client den WINS-Server, um den NetBIOS-Namen dieses Hosts aufzulösen. Sofern dieser Host seinen eigenen

NetBIOS-Namen am selben WINS-Server registriert hat, wird der Benutzer diesen Host auch sehen können.

10.4.5 Bemerkung zu Broadcast-Adressen

Wenn Ihr Netzwerk eine auf 0 basierende Broadcast-Adresse verwendet (zum Beispiel, wenn diese auf 0 endet), dann werden Sie Probleme bekommen. Windows for Workgroups scheint keine 0-Broadcasts zu unterstützen, und Sie werden wahrscheinlich herausfinden, dass das Browsing und die Namensauflösung nicht funktionieren.

10.4.6 Mehrere Interfaces

Samba unterstützt Maschinen mit mehreren Netzwerk-Interfaces. Wenn Sie mehrere Interfaces haben, müssen Sie die Option interfaces in `smb.conf` setzen, um sie zu konfigurieren.

10.4.7 Verwendung des Parameters Remote Announce

Mit dem Parameter remote announce in `smb.conf` können Sie erzwingen, dass all die NetBIOS-Namen eines Netzwerks in einem entfernten Netzwerk bekannt gegeben werden. Die Syntax des Parameters remote announce ist: *remote announce = a.b.c.d [e.f.g.h] ...*
oder *remote announce = a.b.c.d/ARBEITSGRUPPE [e.f.g.h/ARBEITSGRUPPE] ...*
wobei Folgendes gilt:

a.b.c.d* und *e.f.g.h ist entweder die IP-Adresse des LMB (lokalen Master-Browsers) oder die Broadcast-Adresse des entfernten Netzwerks, d.h., der LMB ist unter 192.168.1.10 erreichbar, oder die Adresse wird als 192.168.1.255 angegeben, wobei ein 24-Bit-Netzwerk angenommen wird (255.255.255.0). Wenn die Bekanntgabe an die Broadcast-Adresse des entfernten Netzwerks erfolgt, wird jeder Host diese empfangen. Das macht ziemlich viel „*Lärm*“ im Netz und ist daher nicht erstrebenswert, kann aber erforderlich sein, wenn wir die IP-Adresse des entfernten LMBs nicht kennen.

ARBEITSGRUPPE ist optional und kann entweder unsere eigene Arbeitsgruppe oder die des entfernten Netzwerks sein. Wenn Sie den Arbeitsgruppen-Namen des entfernten Netzwerks verwenden, werden unsere NetBIOS-Maschinen-Namen so aussehen, als ob sie jener Arbeitsgruppe gehörten. Dies kann zu Problemen bei der Namensauflösung führen und sollte vermieden werden.

10.4.8 Verwendung des Parameters Remote Browse Sync

Der Parameter remote browse sync in `smb.conf` wird verwendet, um einem anderen LMB mitzuteilen, dass er seine NetBIOS-Namensliste mit unserem Samba-LMB synchronisieren muss. Dies funktioniert nur, wenn der Samba-Server, der diese Option gesetzt hat, gleichzeitig der LMB in seinem Netzwerk-Segment ist.

Die Syntax des Parameters remote browse sync ist: `remote browse sync = a.b.c.d` wobei `a.b.c.d` entweder die IP-Adresse des entfernten LMBs ist oder die Netzwerk-Broadcast-Adresse des entfernten Netzwerk-Segments.

10.5 WINS — Der „*Windows Internetworking Name Server*“

Die Verwendung von WINS (entweder als Samba-WINS oder als MS Windows NT-Server-WINS) wird wärmstens empfohlen. Jede NetBIOS-Maschine registriert seinen Namen zusammen mit einem „*name_type*“-Wert für jeden der Dienste, die sie zur Verfügung stellt. Die Maschine registriert ihren Namen direkt als eindeutigen Namen (Typ 0x03). Sie registriert ihren Namen auch, wenn sie den LanManager-kompatiblen Server-Dienst ausführt (er wird zur Freigabe von Dateien und Druckern verwendet), indem sie den Server-Namen (Typ 0x20) registriert.

Alle NetBIOS-Namen sind bis zu 15 Zeichen lang. Die Variable „*name_type*“ wird an den Namen angehängt, daher entsteht ein 16-Zeichen-Name. Jeder Name, der kürzer als 15 Zeichen ist, wird mit Leerzeichen bis zum 15. Zeichen aufgefüllt. Daher sind alle NetBIOS-Namen 16 Zeichen lang (inklusive der „*name_type*“-Information).

WINS kann diese 16-Zeichen-Namen bei ihrer Registrierung speichern. Ein Client, der sich am Netzwerk anmelden will, kann den WINS-Server nach einer Liste aller registrierten Namen befragen. Das spart Broadcast-Netzwerkverkehr und beschleunigt die Bearbeitung von Anmeldungen deutlich. Da die Broadcast-Namensauflösung nicht über Netzwerk-Segmente hinweg verwendet werden kann, kann diese Art von Information nur über WINS bereitgestellt werden oder über eine statisch konfigurierte `lmhosts`-Datei, die beim Fehlen von WINS auf allen Clients vorhanden sein muss.

WINS erfüllt auch den Zweck, die Synchronisation von Browse-Listen auf allen LMBs zu erzwingen. Die LMBs müssen ihre Browse-Listen mit dem DMB (Domain Master Browser) synchronisieren, und WINS hilft den LMBs, ihren zugehörigen DMB zu identifizieren. Per Definition funktioniert dies nur innerhalb einer einzelnen Arbeitsgruppe. Beachten Sie, dass der Domain Master Browser nichts mit dem zu tun hat, was als MS Windows NT-Domäne bezeichnet wird. Letzteres ist die Bezeichnung für eine Sicherheitsumgebung, während sich die Bezeichnung DMB nur auf den Master-Controller der Browse-Listen-Informationen bezieht.

WINS arbeitet nur korrekt, wenn der TCP/IP-Protokoll-Stack jedes Clients für die Verwendung der WINS-Server konfiguriert ist. Jeder Client, der nicht für die Verwendung des WINS-Servers konfiguriert ist, verwendet weiterhin eine Broadcast-Namensauflösung, und es kann sein, dass WINS gar nicht von diesem Client erfährt. In jedem Fall werden die Namen von Maschinen, die nicht im WINS registriert sind, nicht von anderen Clients aufgelöst werden können und daher zu Zugriffsproblemen und Fehlern führen.

Um Samba als WINS-Server zu konfigurieren, fügen Sie wins support = yes zum Abschnitt `[global]` ihrer `smb.conf` hinzu.

Um Samba so zu konfigurieren, dass es sich an einem WINS-Server registriert, fügen Sie wins server = a.b.c.d zum Abschnitt `[global]` ihrer `smb.conf` hinzu.

WICHTIG

Verwenden Sie niemals wins support = yes gemeinsam mit wins server = a.b.c.d, besonders nicht mit der eigenen IP-Adresse. Wenn beide Parameter so angegeben werden, wird nmbd den Start verweigern!

10.5.1 Die Konfiguration des WINS-Servers

Sie können entweder einen Samba-Server oder einen Windows NT-Server als WINS-Server einrichten. Um einen Samba-Server als WINS-Server einzurichten, müssen Sie auf dem gewählten Server folgende Zeile zum Abschnitt *[global]* der `smb.conf` hinzufügen:

```
wins support = yes
```

Samba-Versionen vor 1.9.17 hatten diesen Parameter standardmäßig auf „*yes*“ gesetzt. Wenn Sie irgendwelche älteren Samba-Versionen in Ihrem Netzwerk haben, ist es sehr ratsam, diese Installationen auf eine aktuelle Version zu updaten oder zumindest auf all diesen Maschinen den Parameter auf „*no*“ zu setzen.

Maschinen, die mit wins support = yes konfiguriert sind, führen eine Liste aller auf ihnen registrierten NetBIOS-Namen und arbeiten damit als DNS für NetBIOS-Namen.

Es wird wärmstens empfohlen, nur einen WINS-Server einzurichten. Setzen Sie die Option wins support = yes nicht auf mehr als einem Samba-Server.

Um einen Windows NT/200x-Server als WINS-Server einzurichten, installieren und konfigurieren Sie den WINS-Dienst. Konsultieren Sie die Windows NT/200x-Dokumentation für mehr Details zu diesem Thema. Windows NT/200x-WINS-Server können sich untereinander replizieren, was es erlaubt, mehr als einen solchen Server in einer komplexen Subnetz-Umgebung einzurichten. Da Microsoft sich weigert, die Replikationsprotokolle zu dokumentieren, kann Samba derzeit nicht an diesen Replikationen teilnehmen. Es ist möglich, dass zukünftig ein Samba-zu-Samba-WINS-Replikationsprotokoll definiert werden kann, was bedeuten würde, dass mehr als nur eine Samba-Maschine als WINS-Server eingerichtet werden könnte. Derzeit sollte jedoch nur auf einem Samba-Server der Parameter wins support = yes gesetzt sein.

Nachdem der WINS-Server konfiguriert worden ist, müssen Sie sicherstellen, dass alle Maschinen im Netzwerk mit der Adresse dieses WINS-Servers konfiguriert werden. Wenn Ihr WINS-Server eine Samba-Maschine ist, tragen Sie die IP-Adresse der Samba-Maschine im Feld **Primärer WINS Server** der Dialoge **Systemsteuerung->Netzwerk->Protokolle->TCP->WINS Server** von Windows 9x/Me oder Windows NT/200x ein. Um einem Samba-Server die Adresse des WINS-Servers mitzuteilen, fügen Sie die folgende Zeile zum Abschnitt *[global]* ihrer `smb.conf` hinzu:

```
wins server = <Name oder IP-Adresse>
```

wobei <Name oder IP-Adresse> entweder der DNS-Name oder die IP-Adresse des WINS-Servers ist.

Diese Zeile darf nicht in der Datei `smb.conf` des Samba-Servers enthalten sein, der als WINS-Server arbeitet. Wenn Sie sowohl wins support = yes als auch wins server = <name> setzen, wird **nmbd** nicht starten.

Es gibt zwei mögliche Szenarios, um ein Cross-Subnetz-Browsing einzurichten. Das erste behandelt Details der Einrichtung des Cross-Subnetz-Browsings in einem Netzwerk, das Maschinen mit Windows 9x/Me, Samba und Windows NT/200x enthält, die nicht als Mitglieder einer Windows NT-Domäne konfiguriert sind. Das zweite Szenario behandelt die Details der Einrichtung von Cross-Subnetz-Browsing in einem Netzwerk, das NT-Domänen enthält.

10.5.2 WINS-Replikation

Samba-3 erlaubt eine WINS-Replikation, wenn dazu das Utility `wrepld` verwendet wird. Dieses kann derzeit nicht eingesetzt werden, da es sich nach wie vor in der Entwicklung befindet. Sobald es einigermaßen funktioniert, werden wir dazu Manpages erstellen und diesen Abschnitt der Dokumentation erweitern, um Ihnen entsprechende Details zur Verwendung und zu den technischen Hintergründen zur Verfügung zu stellen.

10.5.3 Statische WINS-Einträge

Das Hinzufügen von statischen Einträgen zu Ihrem WINS-Server ist tatsächlich ziemlich einfach. Alles, was Sie tun müssen, ist, eine Zeile zur Datei `wins.dat` hinzuzufügen, üblicherweise in `/usr/local/samba/var/locks` oder `/var/run/samba`.

Einträge in `wins.dat` haben die Form:

```
"NAME#TYPE" TTL ADDRESS+ FLAGS
```

Dabei ist NAME der NetBIOS-Name, TYPE der NetBIOS-Typ, TTL die „*time-to-live*“ als Absolut-Zeit in Sekunden und ADDRESS+ eine oder mehrere Adressen, die mit der Registrierung zusammenhängen; und FLAGS sind die NetBIOS-Flags für die Registrierung.

Ein typischer dynamischer Eintrag sieht so aus:

```
"MADMAN#03" 1055298378 192.168.1.2 66R
```

Um ihn statisch zu machen, muss nur der Wert für TTL auf 0 gesetzt werden:

```
"MADMAN#03" 0 192.168.1.2 66R
```

Obwohl diese Methode nur mit frühen Samba-3-Versionen funktioniert, ist es möglich, dass sie sich in zukünftigen Samba-Versionen verändert, wenn WINS-Replikation hinzugefügt wird.

10.6 Hilfreiche Hinweise

Achten Sie auf die folgenden Hinweise, da diese Punkte bereits für viele Netzwerk-Administratoren zu Stolpersteinen geworden sind.

10.6.1 Windows-Netzwerk-Protokolle

Eine verbreitete Ursache von Browsing-Problemen ist, dass mehrere Netzwerk-Protokolle auf einer MS Windows-Maschine installiert werden.

> WARNUNG
>
> Verwenden Sie nicht mehr als ein Protokoll auf MS Windows-Clients.

Jede NetBIOS-Maschine nimmt alle 15 Minuten an der Wahl des LMB (und des DMB) teil. Eine Anzahl von Auswahl-Kriterien wird verwendet, um die Rangfolge der Maschinen zum Gewinnen dieser Wahl zu bestimmen. Eine Maschine, die Samba ausführt, oder Windows NT, wird bevorzugt, so dass die am ehesten passende Maschine voraussichtlich gewinnen und damit diese Rolle übernehmen wird.

Der Auswahlprozess wird sozusagen über jedes NetBIOS-Netzwerk-Interface „*ausgefochten*“. Im Fall einer Maschine mit Windows 9x/Me, die sowohl TCP/IP als auch IPX installiert hat und NetBIOS über beide Protokolle aktiviert hat, wird die Wahl über beide Protokolle entschieden. Falls, wie es oft passiert, die Maschine mit Windows 9x/Me die einzige mit beiden Protokollen ist, kann der LMB auf dem NetBIOS-Netzwerk-Interface über das IPX-Protokoll gewonnen werden. Samba verliert dann seine LMB-Rolle, da Windows 9x/Me darauf beharrt zu wissen, wer der LMB ist. Samba wird dann seine Funktion als LMB beenden, und daher werden ab da die Browse-Listen-Operationen auf allen Maschinen scheitern, die nur über TCP/IP arbeiten.

Auf Windows 95, 98, 98SE und ME bezieht man sich generell als Windows 9x/Me. Windows NT4, 200x und XP verwenden gemeinsame Protokolle. Diese Systeme werden grob als die Windows-NT-Familie bezeichnet, aber Sie sollten wissen, dass Windows 2000 und XP/2003 neue Protokoll-Erweiterungen einführen, wodurch sich das Verhalten dieser Systeme vom Verhalten von MS Windows NT4 unterscheidet. Allgemein gilt, dass ein Server zur Verwendung der NT4-Protokolle zurückkehrt, wenn er nicht das neuere oder erweiterte Protokoll unterstützt.

Die sicherste Regel von allen, die es zu befolgen gilt, ist: Verwenden Sie nur ein Protokoll!

10.6.2 Die Reihenfolge der Namensauflösung

Die Auflösung von NetBIOS-Namen in IP-Adressen kann mit vielen Methoden erfolgen. Die einzigen Methoden, die NetBIOS-Informationen vom Typ „*name_type*“ bereitstellen können, sind:

- WINS — das beste Werkzeug.
- LMHOSTS — statisch und schwierig zu warten.
- Broadcast — verwendet UDP und kann keine Namen über Segmente hinweg auflösen.

Alternative Möglichkeiten der Namensauflösung sind:

- Statische `/etc/hosts`— schwierig zu warten; fehlende „*name_type*“-Information.
- DNS — ist eine gute Wahl, jedoch fehlt die name_type-Information.

Viele Installationen wollen DNS-Lookups verbieten und den Netzwerk-Verkehr vermeiden, der durch die Broadcast-Namensauflösung entsteht. Der Parameter *name resolve order* ist hier von großer Hilfe. Die Syntax des Parameters *name resolve order* ist: *name resolve order = wins lmhosts bcast host* *oder* *name resolve order = wins lmhosts (eliminiert bcast und host)* Der Standard ist: *name resolve order = host lmhost wins bcast* wobei „*host*“ sich auf die nativen Methoden bezieht, die vom UNIX-System zur Implementation des Funktionsaufrufs gethostbyname() verwendet werden. Dies wird normalerweise über die Dateien `/etc/host.conf`, `/etc/nsswitch.conf` und `/etc/resolv.conf` gesteuert.

10.7 Technischer Überblick über das Browsing

SMB-Netzwerke bieten einen Mechanismus, mit dem Clients auf eine Liste von Maschinen in einem Netzwerk zugreifen können, eine so genannte Browse-Liste. Diese Liste enthält Maschinen, die andere Maschinen im Netzwerk Datei- und/oder Druckdienste anbieten. Daher umfasst diese Liste keine Maschinen, die momentan nicht imstande sind, Serveraufgaben zu erfüllen. Die Browse-Liste wird von allen SMB-Clients intensiv benutzt. Die Konfiguration des SMB-Browsings war für manche Samba-Benutzer problematisch, daher gibt es jetzt dieses Dokument.

MS Windows 2000 und spätere Versionen von Windows, genauso wie Samba-3 und dessen spätere Versionen, können so konfiguriert werden, dass sie NetBIOS-über-TCP/IP nicht verwenden. Wenn sie auf diese Art konfiguriert sind, ist es unumgänglich, dass die Namensauflösung (mittels DNS/LDAP/ADS) korrekt konfiguriert und arbeitsfähig ist. Das Browsing funktioniert nicht, wenn die Namensauflösung von SMB-Maschinen-Namen in IP-Adressen nicht korrekt funktioniert.

Wo NetBIOS-über-TCP/IP aktiviert ist, wird der Einsatz eines WINS-Servers unbedingt empfohlen, um die Namensauflösung zu unterstützen. WINS erlaubt es Clients in anderen Netzwerk-Segmenten, NetBIOS-name_type-Informationen zu beziehen, die von keiner anderen Methode der Namensauflösung bereitgestellt werden können.

10.7.1 Die Unterstützung des Browsings in Samba

Samba unterstützt Browsing. Das Browsing wird von nmbd bereitgestellt und wird auch von Optionen in der Datei `smb.conf` gesteuert. Samba kann als lokaler Master-Browser für eine Arbeitsgruppe arbeiten, und die Fähigkeit, Domänenanmeldungen und Domänenskripts zu unterstützen, ist jetzt verfügbar.

Samba kann auch als Domain Master Browser für eine Arbeitsgruppe arbeiten. Das bedeutet, dass es die Listen der lokalen Master-Browser sammelt und sie zu einer Serverliste für ein gesamtes WAN zusammenfügt. Um es den Clients zu ermöglichen, die Namen, die sie in der Liste finden, auch aufzulösen, wird empfohlen, dass sowohl Samba als auch die Clients einen WINS-Server verwenden.

Konfigurieren Sie Samba nicht als Domänen-Master für eine Arbeitsgruppe, die denselben Namen wie eine NT-Domäne hat. In jedem WAN dürfen Sie immer nur einen Domain Master Browser pro Arbeitsgruppe haben, egal ob es NT, Samba oder sonst ein Typ von Domänen-Master ist, der diesen Dienst anbietet.

ANMERKUNG

nmbd kann als WINS-Server konfiguriert werden, aber es ist nicht notwendig, Samba im Speziellen als WINS-Server zu verwenden. MS Windows NT4, Server oder Advanced Server 200x können als Ihr WINS-Server eingerichtet werden. In einer gemischten NT/200x-Server- und Samba-Umgebung in einem WAN wird empfohlen, dass Sie die MS WINS-Server-Fähigkeiten einsetzen. In einem reinen Samba-Umfeld wird empfohlen, einen und nur einen Samba-Server als WINS-Server zu verwenden.

Um das Browsing zu aktivieren, müssen Sie nmbd wie üblich ausführen, aber müssen auch die Option workgroup `smb.conf` verwenden, um zu bestimmen, welcher Arbeitsgruppe Samba angehören soll.

Samba hat auch eine nützliche Option, um es einem Samba-Server zu ermöglichen, sich selbst für das Browsing in einem anderen Subnetz anzubieten. Es wird empfohlen, diese Option nur für „*ungewöhnliche*“ Zwecke einzusetzen: für Verlautbarungen über das Internet, zum Beispiel. Lesen Sie zu der Option remote announce in der Manpage zu `smb.conf` nach.

10.7.2 Problemlösung

Wenn etwas nicht funktioniert, hilft Ihnen die Datei `log.nmbd`, das Problem zu lokalisieren. Testen Sie einen log level von 2 oder 3, um Probleme zu finden. Beachten Sie auch, dass die aktuelle Browse-Liste üblicherweise in Textform in einer Datei namens `browse.dat` gespeichert wird.

Wenn es nicht funktioniert, sollten Sie noch immer den Servernamen als `\\SERVER` im **Dateimanager** eingeben können, und dieser sollte eine Liste der dort verfügbaren Freigaben

anzeigen.

Manche Anwender haben beobachtet, dass das Browsing scheitert, weil sie die globale Option guest account nicht auf ein gültiges Konto gesetzt haben. Erinnern Sie sich, dass die IPC$-Verbindung, die die Freigaben auflistet, als „*guest*“ hergestellt wird, und dafür brauchen Sie den gültigen guest account.

MS Windows 2000 und spätere Versionen (wie auch Samba) können so konfiguriert werden, dass sie anonymen Zugriff (also mit dem guest account) auf die IPC$-Freigabe verbieten. In diesem Fall verwendet die MS Windows 2000/XP/2003-Maschine den Namen des gerade angemeldeten Benutzers zur Verbindung mit der IPC$-Freigabe. MS Windows 9x/Me-Clients können das nicht und werden dann auch nicht die Ressourcen des Servers browsen können.

Das andere große Problem, das viele Leute haben, ist, dass ihre Broadcast-Adresse, Netmask oder IP-Adresse falsch ist (sie wird mit der Option interfaces in `smb.conf` angegeben).

10.7.3 Cross-Subnetz-Browsing

Seit der Veröffentlichung von Samba 1.9.17 (alpha1) unterstützt Samba die Replikation von Browse-Listen über die Subnetz-Grenzen hinweg. Dieser Abschnitt beschreibt, wie man diese Replikation auf verschiedene Arten einrichtet.

Um Browse-Listen zu sehen, die TCP/IP-Subnetze umspannen (d.h. Netzwerke, die von Routern getrennt sind, die keinen Broadcast-Verkehr weiterleiten), müssen Sie zumindest einen WINS-Server einrichten. Der WINS-Server fungiert als DNS für NetBIOS-Namen. Dies erlaubt die Auflösung von NetBIOS-Namen in IP-Adressen durch eine direkte Abfrage des WINS-Servers. Dies geschieht mittels eines gerichteten UDP-Pakets auf Port 137 der WINS-Server-Maschine. Mit einem WINS-Server ist keine Standard-Namensauflösung erforderlich, die mittels UDP-Broadcasts von der Client-Maschine aus geschehen würde. Das bedeutet, dass Maschinen in einem Subnetz nicht imstande sind, die Namen von Maschinen in einem anderen Subnetz aufzulösen, solange sie keinen WINS-Server verwenden.

Denken Sie daran: Um das Browsing über Subnetze hinweg korrekt funktionieren zu lassen, müssen alle Maschinen, egal ob Windows 95, Windows NT oder Samba, die IP-Adresse einen WINS-Servers mittels DHCP-Server oder manueller Konfiguration erhalten (für Windows 9x/Me und Windows NT/200x/XP erfolgt die Konfiguration in den TCP/IP-Eigenschaften unter den Netzwerkeinstellungen); für Samba erfolgt die Konfiguration in der Datei `smb.conf`.

10.7.3.1 Das Verhalten des Cross-Subnetz-Browsings

Das Cross-Subnetz-Browsing ist ein „*komplizierter Tanz*“, mit vielen bewegten Teilen. Es hat Microsoft einige Jahre gekostet, den Code dafür korrekt zu erstellen, und Samba hängt in einigen Bereichen nach. Samba ist jedoch bei korrekter Konfiguration zum Cross-Subnetz-Browsing imstande.

Nehmen wir an, ein Netzwerk sei so konfiguriert wie im folgenden Cross-Subnetz-Browsing-Beispiel.

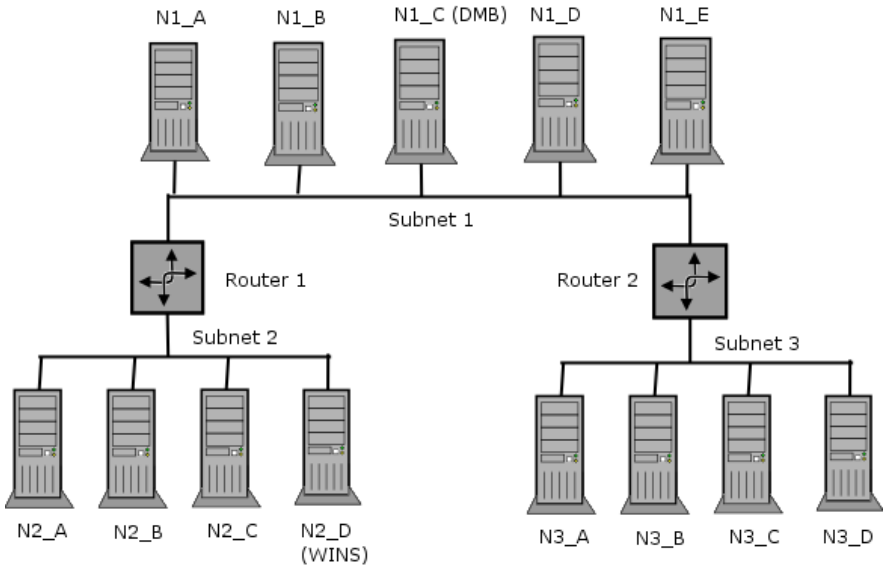


Figure 10.1. Beispiel für das Cross-Subnetz-Browsing

Unser Beispielnetz besteht aus drei Subnetzen (1, 2, 3), die durch zwei Router (R1, R2)verbunden sind, die keine Broadcasts weiterleiten. Subnetz 1 enthält fünf Maschinen, Subnetz 2 vier Maschinen und Subnetz 3 vier Maschinen. Nehmen wir an, dass alle Maschinen so konfiguriert sind, dass sie in der gleichen Arbeitsgruppe sind (der Einfachheit halber). Die Maschine N1_C im Subnetz 1 ist als der Domain Master Browser konfiguriert (d.h., diese Maschine sammelt die Browse-Listen für die Arbeitsgruppe). Die Maschine N2_D ist als der WINS-Server eingerichtet, und alle anderen Maschinen sind so konfiguriert, dass sie ihre jeweiligen NetBIOS-Namen an diesem WINS-Server registrieren.

Wenn diese Maschinen gebootet werden, finden die Wahlen zum Master-Browser in jedem der drei Subnetze statt. Nehmen wir an, dass die Maschine N1_C im Subnetz 1 gewinnt, N2_B im Subnetz 2 und N3_D im Subnetz 3. Diese Maschinen sind sodann als lokale Master-Browser in ihrem jeweiligen Subnetz bekannt. N1_C hat einen Vorteil bei der Wahl zum lokalen Master-Browser im Subnetz 1, da sie als der Domain Master Browser konfiguriert ist.

In jedem der drei Netzwerke werden Maschinen, auf denen Freigaben eingerichtet sind, durch einen Broadcast mitteilen, dass sie diese Dienste anbieten. Der lokale Master-Browser in jedem Subnetz wird diese Broadcasts empfangen und in einem Eintrag festhalten, dass die Maschine diesen Dienst anbietet. Die Liste dieser Einträge ist die Grundlage für die Browse-Liste. Nehmen Sie für diesen Fall an, dass alle Maschinen eingerichtete Freigaben haben, so dass alle Maschinen in der Browse-Liste sind.

Für jedes Netzwerk wird der lokale Master-Browser als „*autoritativ*“ für all die Namen betrachtet, die er durch lokale Broadcasts empfängt. Das rührt daher, dass eine Maschine, die vom LMB über einen lokalen Broadcast gesehen wird, im selben Netzwerk wie der LMB sein muss und daher eine „*vertrauenswürdige*“ und „*überprüfbare*“ Ressource ist. Maschinen

in anderen Netzwerken, von denen die LMBs beim Sammeln der Browse-Listen erfahren, wurden nicht direkt gesehen; diese Einträge werden als „*nicht autoritativ*“ bezeichnet.

An diesem Punkt sehen Browse-Listen wie im nächsten Beispiel aus (dies sind die Maschinen, die Sie in Ihrer Netzwerkumgebung sehen würden, wenn Sie jetzt in einem einzelnen Netzwerk nachsehen würden).

Tabelle 10.1. Subnetz-Browsing Beispiel 1

Subnetz	Browse-Master	Liste
Subnetz1	N1_C	N1_A, N1_B, N1_C, N1_D, N1_E
Subnetz2	N2_B	N2_A, N2_B, N2_C, N2_D
Subnetz3	N3_D	N3_A, N3_B, N3_C, N3_D

An diesem Punkt sind alle Subnetze separat, und keine Maschine wird über die Grenzen eines Subnetzes hinweg gesehen.

Sehen Sie sich nun Subnetz 2 an. Sobald N2_B zum lokalen Master-Browser geworden ist, sucht diese Maschine nach einem DMB, mit dem sie ihre Browse-Liste synchronisieren kann. Das tut sie, indem sie auf dem WINS-Server (N2_D) nach der IP-Adresse fragt, die mit dem NetBIOS-Namen ARBEITSGRUPPE<1B> assoziiert ist. Dieser Name wurde vom DMB (N1_C) auf dem WINS-Server registriert, als der DMB gestartet wurde.

Sobald N2_B die Adresse des DMB kennt, teilt diese Maschine dem DMB mit, dass sie der LMB für das Subnetz 2 ist, indem sie ein *MasterAnnouncement*-Paket als UDP-Paket an den Port 138 sendet. Dann synchronisiert sie sich mit dem DMB, indem sie einen Aufruf namens *NetServerEnum2* durchführt. Das weist den DMB an, all die Servernamen zu senden, über die er Bescheid weiß. Bei Empfang des *MasterAnnouncement*-Pakets setzt der DMB eine Synchronisations-Abfrage an den Absender dieses Pakets ab. Nachdem beide Synchronisationen vollständig erfolgt sind, sehen die Browse-Listen so aus wie in folgender Tabelle:

Tabelle 10.2. Subnetz-Browsing Beispiel 2

Subnetz	Browse-Master	Liste
Subnetz1	N1_C	N1_A, N1_B, N1_C, N1_D, N1_E, N2_A(*), N2_B(*), N2_C(*), N2_D(*)
Subnetz2	N2_B	N2_A, N2_B, N2_C, N2_D, N1_A(*), N1_B(*), N1_C(*), N1_D(*), N1_E(*)
Subnetz3	N3_D	N3_A, N3_B, N3_C, N3_D

Server mit einem folgenden (*) sind nicht-autoritative Namen.

An diesem Punkt sehen die Benutzer, die in ihre Netzwerkumgebungen schauen, im Subnetz 1 oder 2 alle Server auf beiden Subnetzen; Benutzer im Subnetz 3 sehen nach wie vor nur die Server in ihrem eigenen Subnetz.

Dieselbe Abfolge von Ereignissen, die für N2_B geschehen ist, läuft nun für den LMB im Subnetz 3 ab (N3_D). Wenn dieser seine Browse-Liste mit dem DMB (N1_A) synchronisiert, erhält er sowohl die Server-Einträge im Subnetz 1 als auch die im Subnetz 2. Nachdem N3_D

sich mit N1_C synchronisiert hat und vice versa, sehen die Browse-Listen wie im folgenden Beispiel aus.

Tabelle 10.3. Subnetz-Browsing Beispiel 3

Subnetz	Browse-Master	Liste
Subnetz1	N1_C	N1_A, N1_B, N1_C, N1_D, N1_E, N2_A(*), N2_B(*), N2_C(*), N2_D(*), N3_A(*), N3_B(*), N3_C(*), N3_D(*)
Subnetz2	N2_B	N2_A, N2_B, N2_C, N2_D, N1_A(*), N1_B(*), N1_C(*), N1_D(*), N1_E(*)
Subnetz3	N3_D	N3_A, N3_B, N3_C, N3_D, N1_A(*), N1_B(*), N1_C(*), N1_D(*), N1_E(*), N2_A(*), N2_B(*), N2_C(*), N2_D(*)

Server mit einem folgenden (*) sind nicht-autoritative Namen.

An diesem Punkt sehen die Benutzer, die in ihre Netzwerkumgebungen schauen, im Subnetz 1 oder 3 alle Server auf allen Subnetzen; und Benutzer im Subnetz 2 sehen nur die Server in den Subnetzen 1 und 2, aber nicht die im Subnetz 3.

Abschließend wird sich der LMB des Subnetzes 2 (N2_B) mit dem DMB (N1_C) synchronisieren und die fehlenden Server-Einträge erhalten. Wenn dann ein stabiler Zustand erreicht ist (sofern keine Maschinen entfernt oder abgeschaltet werden), sehen die Browse-Listen so aus wie in dieser Tabelle.

Tabelle 10.4. Subnetz-Browsing Beispiel 4

Subnetz	Browse-Master	List
Subnetz1	N1_C	N1_A, N1_B, N1_C, N1_D, N1_E, N2_A(*), N2_B(*), N2_C(*), N2_D(*), N3_A(*), N3_B(*), N3_C(*), N3_D(*)
Subnetzz2	N2_B	N2_A, N2_B, N2_C, N2_D, N1_A(*), N1_B(*), N1_C(*), N1_D(*), N1_E(*), N3_A(*), N3_B(*), N3_C(*), N3_D(*)
Subnetz3	N3_D	N3_A, N3_B, N3_C, N3_D, N1_A(*), N1_B(*), N1_C(*), N1_D(*), N1_E(*), N2_A(*), N2_B(*), N2_C(*), N2_D(*)

Server mit einem folgenden (*) sind nicht-autoritative Namen.

Synchronisationen zwischen dem DMB und den LMBs werden weiter passieren, aber dies sollte ein Vorgang sein, der einen gleich bleibenden Status aufrechterhält und keine Veränderungen herbeiführt.

Wenn Router R1 oder R2 ausfällt, passiert Folgendes:

1. Die Namen von Rechnern auf beiden Seiten der unerreichbaren Netzwerk-Fragmente werden bis zu 36 Minuten lang in den Netzwerkumgebungslisten weitergeführt.

2. Versuche, sich mit diesen unerreichbaren Rechnern zu verbinden, werden scheitern, aber deren Namen werden nicht aus den Netzwerkumgebungslisten entfernt.

#Gtextglqq¿Aber die Freigabe ist von der Befehlszeile (cmd) aus unverzüglich verfügbar. Ist das ein Samba-Problem oder ein Windows-Problem? Wie kann ich es lösen?#Gtextgrqq¿ Hier sind ein paar Möglichkeiten:

[Schlechte Netzwerk-Hardware] Die meisten Probleme mit defekter Hardware haben mit billigen oder defekten Hubs, Routern, Netzwerkkarten (NICs) und schlechter oder fehlerhafter Verkabelung zu tun. Wenn ein Stück Hardware defekt ist, kann das ganze Netzwerk darunter leiden. Schlechte Netzwerk-Hardware kann Datenverluste verursachen. Die meisten Probleme mit Netzwerk-Hardware, jedoch nicht alle, gehen mit auffällig hohem Netzwerk-Verkehr einher. [Der Windows XP WebClient] Eine Reihe von Administratoren haben von ähnlichen Problemen mit langsamem Browsing berichtet und herausgefunden, dass das Problem verschwindet, wenn der Dienst WebClient abgeschaltet wird. Dies sollte auf jeden Fall überprüft werden, weil es eine simple Lösung ist, wenn es funktioniert. [Inkonsistente WINS-Konfiguration] Diese Art von Problem ist gängig, wenn ein Client so konfiguriert worden ist, dass er einen WINS-Server verwenden soll (dies ist eine Einstellung der TCP/IP-Konfiguration) und es keinen WINS-Server im Netzwerk gibt. Dieses Problem kann auch auftreten, wenn es zwar einen WINS-Server gibt, aber Samba nicht zu dessen Verwendung konfiguriert ist. Die Verwendung von WINS wird wärmstens empfohlen, wenn das Netzwerk das NetBIOS-über-TCP/IP-Protokoll verwendet. Wenn die Verwendung von NetBIOS-über-TCP/IP auf allen Clients deaktiviert ist, sollte Samba weder als WINS-Server konfiguriert werden noch zur Verwendung eines solchen. [Falsche DNS-Konfiguration] Dieser Fehler tritt auf, wenn die Verwendung von NetBIOS-über-TCP/IP deaktiviert ist, Active Directory verwendet wird und der DNS-Server fehlerhaft konfiguriert ist. Lesen Sie dazu adsdnstechDNS and Active Directory.

Die Account-Datenbank

Samba-3 besitzt die neue Fähigkeit, gleichzeitig mit mehreren Account-Backends zu arbeiten. Die möglichen neuen Kombinationen von Passwort-Backends ermöglichen Samba-3 eine Flexibilität und Skalierbarkeit, wie sie zuvor nur mit MS Windows Active Directory erreicht werden konnte. Dieses Kapitel beschreibt die neuen Funktionalitäten und zeigt, wie man das Beste aus ihnen herausholt.

Eigenschaften und Vorzüge

Samba-3 bietet folgende Funktionen an, um zu Samba-2.2.x abwärtskompatibel zu sein:

Abwärtskompatible Backends

[Plain Text] Diese Option benutzt nichts weiter als das UNIX/Linux-/etc/passwd-Modell. Bei Betriebssystemen, die Pluggable Authentication Modules (PAM) bieten, werden alle PAM-Module unterstützt. Das Verhalten ist unverändert wie in Samba-2.2.x, und die Protokoll-Beschränkungen, die durch MS Windows-Clients bestehen, treffen gleichermaßen zu. Weitere Informationen über die Einschränkungen bei der Verwendung von Plain-Text-Passwörtern finden Sie im Abschnitt passdbtechTechnischen Informationen. [smbpasswd] Auch diese Option erlaubt weiterhin die Nutzung der Datei smbpasswd, die im simplen ASCII-(Text-)Stil gehalten ist und die verschlüsselten MS Windows-LanMan und NT-Passwörter sowie ein Feld für die Accountinformationen enthält. Diese Art der Passwort-Datenbank enthält keine MS Windows NT/200x-SAM-(Security Account Manager-)Informationen. Diese wären notwendig, um die erweiterten Funktionen für eine umfassendere Zusammenarbeit mit MS Windows NT4/200x-Servern zu bieten. Diese Datenbank sollte nur benutzt werden, um eine Abwärtskompatibilität zu älteren Samba-Versionen zu gewährleisten. Sie wird möglicherweise von zukünftigen Versionen abgelehnt. [ldapsam_compat (Samba-2.2 LDAP Kompatibilität)] Es gibt eine Passwortdatenbank-Option, die weiterhin eine Zusammenarbeit mit einer existierenden OpenLDAP-Datenbank erlaubt, die noch Samba-2.2.x- LDAP-Schemata-Erweiterungen benutzt. Diese vorläufige Option ist als Migrationshilfe gedacht, auch wenn zum jetzigen Zeitpunkt kein zwingender Grund für eine Migration vorliegt. Diese Hilfe wird möglicherweise von zukünftigen Versionen abgelehnt.

Samba-3 führt einige neue Passwortdatenbank-Formen ein.

Neue Backends

[tdbsam] Diese Datenbank ist eine umfangreiche Datenbank für lokale Server. Allerdings eignet sich diese Datenbankmethode nicht für das Aufsetzen von mehreren Domaincontrollern (z.B. ein PDC plus einem oder mehreren BDCs) Die tdbsam-Passwort-Datenbank legt neben den alten smbpasswd-Informationen noch die erweiterten MS Windows NT/200x-SAM-Informationen in binärer Form in der TDB-(Trivial DataBase-)Datei ab. Das Einbeziehen der erweiterten Informationen macht es Samba-3 möglich, die gleichen Account- und System-Zugriffsrechte zu implementieren wie MS Windows NT4/200x-basierende Systeme. Die Einbeziehung der Möglichkeiten von tdbsam ist eine direkte Reaktion auf Benutzernachfragen, die nach einer einfachen Betriebsart ohne den Aufwand von OpenLDAP verlangten. Es wird empfohlen, dieses Verfahren nur bei Standorten bis 250 Benutzern anzuwenden. Für größere Umgebungen wird eine OpenLDAP-basierende Installation wärmstens empfohlen. [ldapsam]

Das Browsing von Freigaben und Verzeichnissen ist sehr langsam

“214 Es gibt nur zwei Maschinen in einem Test-Netzwerk. Eine Maschine ist ein Samba-Server, die andere eine Windows XP-Maschine. Authentifikation und Anmeldungen funktionieren perfekt, aber wenn ich versuche, die Freigaben am Samba-Server zu durchsuchen, wird der Windows XP-Client unbrauchbar. Manchmal reagiert er f“374r einige Minuten nicht. Manchmal antwortet der Windows Explorer und zeigt Dateien und Verzeichnisse ohne Probleme.“215

Die Aufl“366sung von SIDs auf UIDs ist f“374r den korrekten Betrieb von Samba entscheidend. In beiden gezeigten F“344llen, wenn winbindd nicht l“344uft oder nicht erreicht werden kann, ist nur eine lokale SID/UID-Aufl“366sung m“366glich. Sehen Sie sich die Diagramme idmap-sid2uidAufl“366sung von SIDs auf UIDs und idmap-uid2sidAufl“366sung von UIDs auf SIDs an.

[hbt]

[scale=0.5]howto/images/idmap-uid2sid [IDMAP: Aufl“366sung von UIDs auf SIDs]IDMAP: Aufl“366sung von UIDs auf SIDs

#I

#I

10.8.4 Wichtige Bemerkungen zur Sicherheit

Die UNIX- und SMB-Passwort-Verschlüsselungstechniken scheinen auf den ersten Blick ähnlich zu sein. Diese Ähnlichkeit ist jedoch nur sehr oberflächlich. Das UNIX-Schema sendet beim Anmelden Klartext-Passwörter über das Netz. Das ist schlecht. Das SMB-Verschlüsselungsschema sendet niemals das Klartext-Passwort über das Netzwerk, sondern speichert die 16-Byte-Hash-Werte auf der Platte. Das ist auch schlecht. Warum? Weil diese 16-Byte-Hash-Werte ein „*Passwort-Äquivalent*“ sind. Sie können das Passwort des Benutzers nicht daraus ableiten, aber diese Werte könnten möglicherweise in einem modifizierten Client dazu eingesetzt werden, Zugriff auf einen Server zu erlangen. Dies würde einiges technisches Wissen auf Seiten des Angreifers voraussetzen, ist jedoch definitiv möglich. Sie sollten daher die gespeicherten Daten, egal welche Datenbank Sie benutzen (smbpasswd, LDAP, MYSQL), so behandeln, als ob diese Daten die Klartext-Passwörter all Ihrer Benutzer enthielten. Diese Inhalte müssen geheim gehalten werden, und die Datei sollte dementsprechend geschützt werden.

Idealerweise würden wir ein Passwort-Schema bevorzugen, das Klartext-Passwörter weder im Netz noch auf der Festplatte verwendet. Dies ist unglücklicherweise nicht verfügbar, da Samba darauf beschränkt ist, kompatibel mit anderen SMB-Systemen (Windows NT, Windows for Workgroups, Windows 9x/Me) sein zu müssen.

Windows NT 4.0 Service Pack 3 hat die Standard-Einstellung geändert, so dass Klartext-Passwörter nicht mehr über das Netzwerk gesendet werden. Dies macht die Verwendung verschlüsselter Passwörter notwendig bzw. das Editieren der Windows NT-Registrierung, um Klartext-Passwörter wieder zu aktivieren.

Die folgenden Versionen von MS Windows unterstützen NICHT die vollständigen Domänen-Sicherheitsprotokolle, obwohl sie sich an einer Domäne anmelden können:

- MS DOS Network Client 3.0 mit installiertem „*basic network redirector*“
- Windows 95 mit installiertem „*network redirector update*“
- Windows 98 [Second Edition]
- Windows Me

ANMERKUNG

MS Windows XP Home hat keine Einrichtungen, um Domänen-Mitglied zu werden, und kann nicht an Domänen-Anmeldungen teilnehmen.

Die folgenden Versionen von MS Windows unterstützen die vollständigen Domänen-Sicherheitsprotokolle.

- Windows NT 3.5x
- Windows NT 4.0
- Windows 2000 Professional
- Windows 200x Server/Advanced Server
- Windows XP Professional

Alle aktuellen Microsoft SMB/CIFS-Clients unterstützen die Authentifikation über den hier beschriebenen SMB-Challenge/Response-Mechanismus. Das Aktivieren der Klartext-Authentifikation deaktiviert die Fähigkeit des Clients nicht, an verschlüsselter Authentifikation teilzunehmen. Stattdessen erlaubt dies dem Client, entweder Klartext- oder verschlüsselte Passwörter zu verwenden.

MS Windows-Clients puffern nur das verschlüsselte Passwort. Wo Klartext-Passwörter durch den entsprechenden Registrierungseintrag aktiviert wurden, wird das Klartext-Passwort nie gepuffert. Das bedeutet, dass im Fall einer getrennten Netzwerk-Verbindung nur das gepufferte (verschlüsselte) Passwort an den Server gesendet wird, um einen automatischen Wiederaufbau der Verbindung zu erzielen. Wenn der Server keine verschlüsselten Passwörter unterstützt, wird dies scheitern. Die Verwendung verschlüsselter Passwörter wird dringend empfohlen.

10.8.4.1 Vorteile verschlüsselter Passwörter

- Es werden keine Klartext-Passwörter über das Netzwerk versandt. Jemand, der einen Netzwerk-Sniffer verwendet, kann keine an den SMB-Server gesandten Passwörter abhören und aufzeichnen.
- Es werden keine Klartext-Passwörter auf Festplatten oder im RAM abgelegt.
- Windows NT mag es nicht, mit einem Server zu kommunizieren, der keine verschlüsselten Passwörter unterstützt. Es wird sich weigern, den Server zu durchsuchen

(browsing), wenn der Server auch noch im User-Level-Sicherheitsmodus läuft. NT wird darauf bestehen, den Benutzer bei jeder Verbindung nach einem Passwort zu fragen, was sehr lästig ist. Das Einzige, was man dagegegen tun kann, ist die Verwendung der SMB-Verschlüsselung.

- Die Unterstützung verschlüsselter Passwörter erlaubt das automatische Wiederverbinden von Freigaben (Ressourcen).
- Verschlüsselte Passwörter sind unbedingt notwendig für den PDC/BDC-Betrieb.

10.8.4.2 Vorteile nichtverschlüsselter Passwörter

- Es werden keine Klartext-Passwörter auf Festplatten oder im RAM abgelegt.
- Es wird dieselbe Passwort-Datei wie für andere Unix-Dienste, z.B. FTP oder Login, verwendet.
- Es werden andere Dienste (wie Telnet und FTP) verwendet, die Klartext-Passwörter über das Netz senden, daher ist deren Versand für SMB keine so wichtige Angelegenheit mehr.

10.8.5 Die Zuordnung von Benutzer-Identifiern (UIDs) zwischen MS Windows und UNIX

Jede Operation in UNIX/Linux erfordert einen Benutzer-Identifier (UID), genauso wie sie unter MS Windows NT4/200x einen Sicherheits-Identifier (SID) erfordert. Samba stellt zwei Verfahren zur Verfügung, um einen Windows-Benutzer einem UNIX/Linux-UID zuzuweisen.

Als Erstes brauchen alle Samba-SAM-Konten (Security-Account-Manager-Datenbank) eine UNIX/Linux-UID, der das jeweilige Konto zugewiesen wird. Da Benutzer der Konten-Datenbank hinzugefügt werden, ruft Samba das add user script-Interface auf, um das Konto dem Betriebssystem, unter dem Samba läuft, hinzuzufügen. Grundsätzlich brauchen alle Konten in der lokalen SAM ein lokales Benutzerkonto.

Die zweite Möglichkeit, die Zuweisung von Windows-SIDs an UNIX-UIDs zu erzielen, nutzt die Parameter *idmap uid* und *idmap gid* in `smb.conf`. Bitte lesen Sie die Manpage für Informationen zu diesen Parametern. Sie sind von grundlegender Bedeutung, wenn man Benutzer von einem enfernten SAM-Server mappen muss.

10.8.6 Das Zuweisen gemeinsamer UIDs/GIDs auf verteilten Maschinen

Samba-3 hat eine spezielle Einrichtung, die es ermöglicht, identische UIDs und GIDs auf allen Servern eines verteilten Netzwerks aufrechtzuerhalten. Ein verteiltes Netzwerk ist ein Netzwerk, in dem ein PDC, ein oder mehrere BDCs und/oder ein oder mehrere Domänen-Mitgliedsserver existieren. Warum ist dies wichtig? Es ist wichtig, wenn Dateien über mehr als nur ein Protokoll (z.B. NFS) im Netz bereitgestellt werden und wenn Benutzer Dateien mit Werkzeugen wie **rsync** zwischen UNIX/Linux-Systemen kopieren.

Die spezielle Einrichtung wird mit einem Parameter namens *`idmap backend`* aktiviert. Die Standard-Einstellung für diesen Parameter ist ein leerer String. Technisch ist es möglich,

ein LDAP-Backend für UIDs und GIDs zu verwenden. Dies macht dann am meisten Sinn, wenn es in Netzwerk-Konfigurationen verwendet wird, die auch LDAP für das SAM-Backend verwenden. Sehen Sie sich dazu dieses Beispiel an.

Beispiel 10.8.1. Beispielkonfiguration mit dem LDAP-idmap-Backend

```
[global]
        idmap backend = ldap:ldap://ldap-server.quenya.org:636
        idmap backend = ldap:ldaps://ldap-server.quenya.org
```

Ein Netzwerk-Administrator, der ernsthaft LDAP-Backends verwenden will, wird früher oder später auf die exzellente Arbeit von PADL Software stoßen. PADL <`http://www.padl.com`> hat eine Reihe von Werkzeugen produziert und als OpenSource veröffentlicht, die von Interesse sein könnten. Diese Werkzeuge enthalten:

- *nss_ldap:* Ein LDAP-Name-Service-Switch-Modul, um native Namensdienst-Unterstützung für AIX, Linux, Solaris und andere Betriebssysteme anzubieten. Dieses Werkzeug kann zum zentralen Speichern und Beziehen von UIDs/GIDs verwendet werden.
- *pam_ldap:* Ein PAM-Modul, das LDAP-Integration für die UNIX/Linux-System-Authentifikation bietet.
- *idmap_ad:* Ein IDMAP-Backend, das das Schema „*Microsoft Services for UNIX RFC 2307*“ unterstützt, das unter <`http://www.padl.com/download/xad_oss_plugins.tar.gz`> zu finden ist.

10.9 Werkzeuge zur Verwaltung von Konten

Samba enthält zwei Werkzeuge zur Verwaltung von Benutzer- und Maschinen-Konten. Diese Werkzeuge sind **smbpasswd** und **pdbedit**.

10.9.1 Der Befehl *smbpasswd*

Das Hilfsprogramm **smbpasswd** ähnelt den Programmen **passwd** oder **yppasswd**. Es wartet die beiden 32 Byte großen Passwort-Felder im passdb-Backend.

smbpasswd arbeitet in einem Client-Server-Modus, wo es den lokalen smbd kontaktiert, um das Passwort des Benutzers selbst zu ändern. Dies hat enorme Vorteile.

smbpasswd hat die Fähigkeit, Passwörter auf Windows NT-Servern zu ändern (dies funktioniert nur, wenn die Anfrage an den NT-PDC gesendet wird, wenn man das Passwort eines Domänen-Benutzers ändert).

smbpasswd kann für Folgendes verwendet werden:

- *Hinzufügen* von Benutzer- oder Maschinen-Konten
- *Löschen* von Benutzer- oder Maschinen-Konten
- *Aktivieren* von Benutzer- oder Maschinen-Konten

- *Deaktivieren* von Benutzer- oder Maschinen-Konten
- *Auf-NULL-Setzen* von Benutzer-Passwörtern
- *Verwalten von Domänen-Vertrauenskonten*

Um smbpasswd als normaler Benutzer auszuführen, tippen Sie einfach:

```
$ smbpasswd
Old SMB password: secret
```

Anstatt *secret*, geben Sie hier den alten Wert an oder drücken einfach Enter, falls es kein altes Passwort gibt.

```
New SMB Password: new secret
Repeat New SMB Password: new secret
```

Wenn der alte Wert nicht mit dem aktuell für den Benutzer gespeicherten Wert übereinstimmt oder die beiden neuen Werte nicht zusammenpassen, wird das Passwort nicht geändert.

Von einem normalen Benutzer aufgerufen, erlaubt der Befehl dem Benutzer nur, das eigene Passwort zu ändern.

Wird der Befehl von root ausgeführt, akzeptiert **smbpasswd** ein optionales Argument, das den Benutzer angibt, dessen Passwort Sie verändern wollen. Mit root-Rechten ausgeführt, fragt **smbpasswd** nicht nach dem alten Passwort (bzw. prüft es auch nicht) und erlaubt daher dem Benutzer root, Passwörter für Benutzer zu setzen, die ihr Passwort vergessen haben.

smbpasswd wurde so entworfen, dass seine Arbeitsweise derjenigen ähnelt, die Benutzern der Befehle **passwd** oder **yppasswd** vertraut ist. Obwohl es für die administrative Anwendung entworfen worden ist, bietet dieses Werkzeug die wichtige Fähigkeit, auf Benutzer-Ebene Passwörter zu ändern.

Lesen Sie die Manpage (die definitive Referenz) für mehr Details zur Verwendung von **smbpasswd**.

10.9.2 Der Befehl *pdbedit*

pdbedit ist ein Werkzeug, das nur von root verwendet werden kann. Es wird zur Verwaltung des passdb-Backends verwendet. **pdbedit** kann für Folgendes verwendet werden:

- Hinzufügen, Löschen oder Ändern von Benutzerkonten
- Auflisten von Benutzerkonten
- Migrieren von Benutzerkonten

Das Werkzeug **pdbedit** ist das einzige Werkzeug, das die Sicherheits- und Richtlinien-Einstellungen der Konten verwalten kann. Es kann sowohl alle Operationen durchführen, die smbpasswd beherrscht, als auch ein Super-Set davon.

Ein besonders wichtiger Zweck von **pdbedit** ist es, die Migration von Konten-Informationen von einem passdb-Backend in ein anderes zu erlauben. Lesen Sie dazu auch den Abschnitt zum XML-Backend in diesem Kapitel.

Das Folgende ist ein Beispiel für die Benutzer-Konten-Information, die in einem tdbsam-passdb-Backend gespeichert ist. Diese Liste wurde so erzeugt:

```
$ pdbedit -Lv met
UNIX username:        met
NT username:
Account Flags:        [UX         ]
User SID:             S-1-5-21-1449123459-1407424037-3116680435-2004
Primary Group SID:    S-1-5-21-1449123459-1407424037-3116680435-1201
Full Name:            Melissa E Terpstra
Home Directory:       \\frodo\met\Win9Profile
HomeDir Drive:        H:
Logon Script:         scripts\logon.bat
Profile Path:         \\frodo\Profiles\met
Domain:               MITTELERDE
Account desc:
Workstations:         melbelle
Munged dial:
Logon time:           0
Logoff time:          Mon, 18 Jan 2038 20:14:07 GMT
Kickoff time:         Mon, 18 Jan 2038 20:14:07 GMT
Password last set:    Sat, 14 Dec 2002 14:37:03 GMT
Password can change:  Sat, 14 Dec 2002 14:37:03 GMT
Password must change: Mon, 18 Jan 2038 20:14:07 GMT
```

pdbedit erlaubt die Migration von Authentifikationsdatenbanken (entspricht Konten-Datenbanken) von einem Backend in ein anderes. Um zum Beispiel Konten von einem alten `smbpasswd`-Backend in ein *`tdbsam`*-Backend zu migrieren, tun Sie Folgendes:

1. Setzen Sie den Parameter passdb backend = tdbsam, smbpasswd.

2. Führen Sie dies aus:

   ```
   root# pdbedit -i smbpasswd -e tdbsam
   ```

3. Jetzt entfernen Sie den Wert *`smbpasswd`* aus dem Parameter passdb backend in `smb.conf`.

10.10 Passwort-Backends

Von allen heute verfügbaren SMB/CIFS-Server-Technologien bietet Samba die größte Flexibilität im Design der Konten-Datenbank-Backends. Die Flexibilität wird unmittelbar sichtbar, sobald man beginnt, diese Fähigkeiten zu erforschen.

Es ist nicht nur möglich, mehrere verschiedene Passwort-Backends zu spezifizieren, sondern auch mehrere Backends desselben Typs. Ein Beispiel für die Verwendung zwei verschiedener tdbsam-Datenbanken sähe so aus:

```
        passdb backend = tdbsam:/etc/samba/passdb.tdb \
tdbsam:/etc/samba/old-passdb.tdb
```

10.10.1 Klartext

Ältere Samba-Versionen bezogen die Benutzer-Informationen aus der UNIX-Benutzer-Datenbank und eventuell ein paar weiteren Feldern aus der Datei `/etc/samba/smbpasswd` oder `/etc/smbpasswd`. Wenn die Passwort-Verschlüsselung deaktiviert ist, werden überhaupt keine SMB-spezifischen Daten gespeichert. Stattdessen werden alle Operationen auf die Art durchgeführt, in der das Wirtsbetriebssystem auf seine Datenbank `/etc/passwd` zugreift. Auf Linux-Systemen geschieht dies beispielsweise via PAM.

10.10.2 smbpasswd — Datenbank für verschlüsselte Passwörter

Traditionellerweise wurden Benutzer-Konten-Informationen wie Benutzername, LM/NT-Passwort-Hashes, Passwort-Änderungszeiten und Konten-Flags in der Datei `smbpasswd(5)` gespeichert. Es gibt einige Nachteile bei diesem Ansatz, besonders für Installationen mit einer großen Anzahl von Benutzern (wir sprechen hier von Tausenden...).

- Das erste Problem ist, dass alle Suchen („*Lookups*“) sequenziell ausgeführt werden müssen. Dadurch, dass durchschnittlich zwei Lookups pro Domänen-Anmeldung ausgeführt werden (einer für die normale Verbindung wie beim Verbinden eines Netzwerk-Laufwerks oder -Druckers) ist dies performance-mäßig ein Flaschenhals für große Installationen. Was hier gebraucht wird, ist ein Ansatz mit Indizes, wie er in Datenbanken verwendet wird.
- Das zweite Problem ist, dass Administratoren, die eine smbpasswd-Datei auf mehr als einen Samba-Server replizieren wollen, externe Werkzeuge wie **rsync(1)** und **ssh(1)** verwenden mussten, und eigene, haus-interne Skripts geschrieben haben.
- Zuletzt lässt die Menge an Informationen, die in einem smbpasswd-Eintrag gespeichert wird, keinen Platz für weitere Attribute, wie z.B. ein Home-Verzeichnis, das Ablaufdatum des Passworts oder auch nur für einen Relative Identifier (RID).

Als Schlussfolgerung aus diesen Mängeln wurde ein robusteres Hilfsmittel entwickelt, mit dem smbd Benutzer-Attribute speichern kann. Die API, die den Zugriff auf Benutzer-Konten definiert, wird üblicherweise als das samdb-Interface bezeichnet (davor wurde sie als die passdb-API bezeichnet, und im Samba-CVS-Tree wird sie das immer noch).

Samba bietet eine erweiterte Auswahl an passdb-Backends, die die Mängel der smbpasswd-Klartext-Datenbank beseitigen. Diese sind tdbsam, ldapsam und xmlsam. Aus diesen dreien

wird ldapsam dasjenige sein, das für große Firmen- oder Unternehmensinstallationen von größtem Interesse ist.

10.10.3 tdbsam

Samba kann Daten von Benutzer- und Maschinen-Konten in einer „*TDB*“ (Trivial Database) abspeichern. Die Verwendung dieses Backends erfordert keine weitere Konfiguration. Dieses Backend wird für neue Installationen empfohlen, die kein LDAP benötigen.

Als generelle Richtlinie empfiehlt das Samba-Team, das tbd-Backend nicht in Installationen einzusetzen, die 250 oder mehr Benutzer haben. Außerdem unterstützt tdbsam kein Replikationsprotokoll für Samba-PDC- und -BDC-Installationen. In solchen Fällen ist die Verwendung von ldapsam ratsam.

Die Empfehlung eines Limits von 250 Benutzern basiert einfach darauf, dass dies üblicherweise eine Installation mit gerouteten Netzwerken ist, die sich eventuell auch über mehrere physische Standorte erstreckt. Das Samba-Team hat bis dato noch nicht die Skalierbarkeitslimits der tdbsam-Architektur in Bezug auf Performance festgelegt.

10.10.4 ldapsam

Es gibt ein paar Punkte zu erwähnen, die ldapsam nicht anbietet. Die LDAP-Unterstützung, auf die sich diese Dokumentation bezieht, enthält nicht:

- Eine Einrichtung, um Benutzer-Konten-Informationen von einem Windows 200x Active Directory Server zu beziehen
- Eine Einrichtung, um /etc/passwd zu ersetzen

Der zweite Punkt kann durch die Verwendung von LDAP-NSS- und PAM-Modulen abgedeckt werden. GPL-Versionen dieser Bibliotheken können von PADL Software <`http://www.padl.com/`> bezogen werden. Mehr Informationen zur Konfiguration dieser Pakete finden Sie in dem Buch *LDAP, System Administration*; von Gerald Carter, das im O'Reilly Verlag erschienen ist. Lesen Sie dort Kapitel 6: Replacing NIS <`http://safari.oreilly.com/?XmlId=1-56592-491-6`>.

Dieses Dokument beschreibt, wie man ein LDAP-Verzeichnis dazu verwendet, Samba-Benutzerkonten-Informationen abzuspeichern, die traditionell in der Datei smbpasswd(5) abgelegt wurden. Es wird angenommen, dass Sie die LDAP-Konzepte vom Grundsatz her verstehen und bereits einen funktionierenden Verzeichnis-Server installiert haben. Für mehr Informationen zu LDAP-Architektur und -Verzeichnissen besuchen Sie bitte folgende Seiten:

- OpenLDAP <`http://www.openldap.org/`>
- Sun iPlanet Directory Server <`http://iplanet.netscape.com/directory`>

Zwei weitere Samba-Ressourcen, die vielleicht hilfreich sein können, sind:

- Das Samba-PDC-LDAP-HOWTO <`http://www.unav.es/cti/ldap-smb/ldap-smb-3-howto.html`>, verwaltet von Ignacio Coupeau

- Die NT-Migrations-Skripten von IDEALX <http://samba.idealx.org/>, die dafür ausgelegt sind, Benutzer und Gruppen in einer solchen Samba-LDAP-Domänencontroller-Konfiguration zu verwalten.

10.10.4.1 Unterstützte LDAP-Server

Der LDAP ldapsam-Code wurde unter Verwendung der OpenLDAP 2.0 und 2.1 Server- und Client-Libraries entwickelt und getestet. Derselbe Code sollte mit Netscapes Directory Server und Client SDK arbeiten. Jedoch gibt es Compile-Fehler und Bugs. Diese sollten nicht schwierig zu beheben sein. Bitte senden Sie uns Fixes mit dem in Reporting Bugs beschriebenen Vorgehen.

10.10.4.2 Schema und Verhältnis zum RFC 2307-posixAccount

Samba-3.0 enthält die notwendige Schema-Datei für OpenLDAP 2.0 in `examples/LDAP/samba.schema`. Die sambaSamAccount-Objekt-Klasse sehen Sie hier:

```
objectclass (1.3.6.1.4.1.7165.2.2.6 NAME 'sambaSamAccount' SUP top AUXILIARY
    DESC 'Samba-3.0 Auxiliary SAM Account'
    MUST ( uid $ sambaSID )
    MAY  ( cn $ sambaLMPassword $ sambaNTPassword $ sambaPwdLastSet $
           sambaLogonTime $ sambaLogoffTime $ sambaKickoffTime $
           sambaPwdCanChange $ sambaPwdMustChange $ sambaAcctFlags $
           displayName $ sambaHomePath $ sambaHomeDrive $ sambaLogonScript $
           sambaProfilePath $ description $ sambaUserWorkstations $
           sambaPrimaryGroupSID $ sambaDomainName ))
```

Die Datei `samba.schema` wurde für OpenLDAP 2.0/2.1 formatiert. Das Samba-Team besitzt den OID-Space, der vom obigen Schema benutzt wird, und empfiehlt dessen Verwendung. Wenn Sie das Schema für die Verwendung mit Netscape-DS übersetzen, senden Sie die modifzierte Schema-Datei bitte als Patch an jerry@samba.org <mailto:jerry@samba.org>.

Genauso wie die Datei smbpasswd zum Speichern von Informationen gedacht ist, die über die in der Datei `/etc/passwd` gespeicherten Informationen hinausgehen, ist das Objekt sambaSamAccount zur Ergänzung der UNIX-Benutzerkonten-Information gedacht. Ein sambaSamAccount ist eine `AUXILIARY`-Objektklasse, so dass sie zur Erweiterung existierender Benutzer-Konten-Information im LDAP-Verzeichnis verwendet werden kann. Es gibt jedoch einige Felder (z.B. uid), die mit der posixAccount-Objektklasse überlappen, die in RFC2307 beschrieben wird. Dies ist vom Design her so vorgesehen.

Um die gesamte Benutzer-Konten-Information (UNIX und Samba) in dem Verzeichnis speichern zu können, ist es notwendig, die beiden Objektklassen sambaSamAccount und posixAccount in Kombination zu verwenden. Jedoch wird smbd die Benutzer-Konten-Information nach wie vor über die Standard-C-Bibliotheksaufrufe beziehen (z.B. getpwnam() und andere). Das bedeutet, dass der Samba-Server auch die LDAP-NSS-Bibliothek installiert haben muss und diese korrekt funktionieren muss. Diese Trennung von Informationen macht

es möglich, alle Samba-Informationen in LDAP zu speichern, aber weiterhin die UNIX-Konten-Informationen in NIS zu verwalten, während das Netzwerk in eine vollständige LDAP-Infrastruktur überführt wird.

10.10.4.3 OpenLDAP-Konfiguration

Um Unterstützung für das Objekt sambaSamAccount in einem OpenLDAP-Verzeichnis zu einzubinden, kopieren Sie als Erstes die Datei samba.schema in das Konfigurationsverzeichnis von slapd. Die Datei samba.schema kann im Verzeichnis `examples/LDAP` in der Samba-Quelldistribution gefunden werden.

```
root# cp samba.schema /etc/openldap/schema/
```

Als Nächstes binden Sie die Datei `samba.schema` in `slapd.conf` ein. Das Objekt sambaSamAccount enthält zwei Attribute, die auf anderen Schema-Dateien basieren. Das Attribut *`uid`* wird in `cosine.schema` definiert und das Attribut *`displayName`* in der Datei `inetorgperson.schema`. Beide müssen vor der Datei `samba.schema` eingebunden werden.

```
## /etc/openldap/slapd.conf

## schema files (core.schema is required by default)
include             /etc/openldap/schema/core.schema

## needed for sambaSamAccount
include            /etc/openldap/schema/cosine.schema
include            /etc/openldap/schema/inetorgperson.schema
include            /etc/openldap/schema/nis.schema
include            /etc/openldap/schema/samba.schema
....
```

Es wird empfohlen, dass Sie einige Indizes von den wichtigsten Attributen pflegen, um Suchen nach sambaSamAccount-Objektklassen zu beschleunigen (und eventuell auch posixAccount und posixGroup). Zum Beispiel:

```
## Zu pflegende Indizes
## von LDAP benötigt
index objectclass             eq

index cn                      pres,sub,eq
index sn                      pres,sub,eq
## zur Unterstützung von pdb_getsampwnam
index uid                     pres,sub,eq
## zur Unterstützung von pdb_getsambapwrid()
index displayName             pres,sub,eq
```

```
## entfernen Sie hier die Kommentarzeichen,
## wenn Sie auch posixAccount- und
## posixGroup-Einträge im Verzeichnis verwalten
##index uidNumber               eq
##index gidNumber               eq
##index memberUid               eq

index   sambaSID              eq
index   sambaPrimaryGroupSID  eq
index   sambaDomainName       eq
index   default               sub
```

Legen Sie den neuen Index an, indem Sie dies ausführen:

```
root# ./sbin/slapindex -f slapd.conf
```

Vergessen Sie nicht, slapd nach diesen Änderungen neu zu starten:

```
root# /etc/init.d/slapd restart
```

10.10.4.4 Das Initialisieren der LDAP-Datenbank

Bevor Sie Konten der LDAP-Datenbank hinzufügen können, müssen Sie die Konten-Container anlegen, in denen diese gespeichert werden sollen. Die folgende LDIF-Datei sollte so editiert werden, dass sie Ihrem Bedarf entspricht (DNS-Einträge usw.):

```
# Organisation fuer Samba-Basis
dn: dc=quenya,dc=org
objectclass: dcObject
objectclass: organization
dc: quenya
o: Quenya Org Netzwerk
description: Das Samba-3 Netzwerk LDAP Beispiel

# Organisatorische Rolle fuer Verzeichnisverwaltung
dn: cn=Manager,dc=quenya,dc=org
objectclass: organizationalRole
cn: Manager
description: Verzeichnis Manager

# Einrichten des Benutzer-Containers
dn: ou=People,dc=quenya,dc=org
objectclass: top
objectclass: organizationalUnit
```

```
ou: People

# Einrichten des Administrators fuer die People-OU
dn: cn=admin,ou=People,dc=quenya,dc=org
cn: admin
objectclass: top
objectclass: organizationalRole
objectclass: simpleSecurityObject
userPassword: {SSHA}c3ZM9tBaBo9autm1dL3waDS21+JSfQVz

# Einrichten des Gruppen-Containers
dn: ou=Groups,dc=quenya,dc=org
objectclass: top
objectclass: organizationalUnit
ou: Groups

# Einrichten des Administrators fuer die Gruppen-OU
dn: cn=admin,ou=Groups,dc=quenya,dc=org
cn: admin
objectclass: top
objectclass: organizationalRole
objectclass: simpleSecurityObject
userPassword: {SSHA}c3ZM9tBaBo9autm1dL3waDS21+JSfQVz

# Einrichten des Computer-Containers
dn: ou=Computers,dc=quenya,dc=org
objectclass: top
objectclass: organizationalUnit
ou: Computers

# Einrichten des Administrators fuer die Computer-OU
dn: cn=admin,ou=Computers,dc=quenya,dc=org
cn: admin
objectclass: top
objectclass: organizationalRole
objectclass: simpleSecurityObject
userPassword: {SSHA}c3ZM9tBaBo9autm1dL3waDS21+JSfQVz
```

Das oben gezeigte userPassword sollte mittels **slappasswd** generiert werden.

Der folgende Befehl lädt dann den Inhalt der LDIF-Datei in die LDAP-Datenbank:

```
$ slapadd -v -l initldap.dif
```

Vergessen Sie nicht, Ihren LDAP-Server sowohl mit einer adäquaten ACL zu versehen als auch mit einem Administrator-Passwort.

ANMERKUNG

Bevor Samba auf den LDAP-Server zugreifen kann, müssen Sie das LDAP-Administrator-Passwort in die Samba-3-Datenbank `secrets.tdb` speichern:

```
root# smbpasswd -w secret
```

10.10.4.5 Die Konfiguration von Samba

Folgende Parameter sind nur dann in smb.conf verfügbar, wenn Ihre Version von Samba mit LDAP-Unterstützung kompiliert worden ist. Samba wird automatisch so konfiguriert, wenn die LDAP-Bibliotheken vorgefunden werden.

LDAP-bezogene smb.conf-Optionen sind: passdb backend = ldapsam:url, ldap admin dn, ldap delete dn, ldap filter, ldap group suffix, ldap idmap suffix, ldap machine suffix, ldap passwd sync, ldap ssl, ldap suffix und ldap user suffix.

Diese Parameter werden in der Manpage zu `smb.conf` beschrieben, dies wird hier nicht wiederholt. Wir zeigen jedoch eine Beispieldatei `smb.conf` für die Verwendung mit einem LDAP-Verzeichnis.

10.10.4.6 Das Management von Benutzern und Gruppen

Da Benutzerkonten mit der sambaSamAccount-Objektklasse verwaltet werden, sollten Sie Ihre bereits existierenden Administrationswerkzeuge so modifizieren, dass sie mit sambaSamAccount-Attributen umgehen können.

Maschinenkonten werden mit der sambaSamAccount-Objektklasse verwaltet, genauso wie Benutzerkonten. Es ist jedoch Ihnen überlassen, diese Konten in einem anderen Zweig Ihres LDAP-Namensraums zu speichern. Sie sollten „*ou=Groups,dc=quenya,dc=org*“ zum Speichern von Gruppen und „*ou=People,dc=quenya,dc=org*“ zum Speichern von Benutzern verwenden. Konfigurieren Sie nur Ihr NSS und PAM dementsprechend (üblicherweise in der Datei `/etc/openldap/sldap.conf`).

In Samba-3 basiert die Gruppenverwaltung auf den POSIX-Gruppen. Das bedeutet, dass Samba die posixGroup-Objektklasse verwendet. Derzeit gibt es keine NT-artige Gruppenverwaltung (globale und lokale Gruppen). Samba-3 kennt nur `Domänen-Gruppen`, und unterstützt, im Unterschied zu MS Windows 2000 und Active Directory, keine verschachtelten Gruppen.

Beispiel 10.10.1. Konfiguration mit LDAP

```
[global]
        security = user
        encrypt passwords = yes
        netbios name = MORIA
        workgroup = NOLDOR
# ldap-bezogene Parameter
# Definieren der DN, mit der die Verbindung zu den Verzeichnis-Servern hergestellt wird
# Das Passwort für diese DN wird nicht in smb.conf gespeichert. Es muss mit
# 'smbpasswd -w secretpw'
# in der Datei secrets.tdb gespeichert werden. Wenn sich der Wert „ldap admin dn“ ändert,
# muss dieses Passwort zurückgesetzt werden.
        ldap admin dn = cn=Manager,dc=quenya,dc=org"
# Definieren der SSL-Option beim Verbinden zum Verzeichnis
# ('off', 'start tls', oder 'on' (default))
        ldap ssl = start tls
# syntax: passdb backend = ldapsam:ldap://server-name[:port]
        passdb backend = ldapsam:ldap://frodo.quenya.org
# smbpasswd -x löscht den ganzen dn-Eintrag
        ldap delete dn = no
# Maschinen- und Benutzer-Suffix, die an das Basis-Suffix angehängt werden.
# Schreibweise OHNE Anführungszeichen. NULL-Suffixe als Standard
        ldap user suffix = ou=People
        ldap group suffix = ou=Groups
        ldap machine suffix = ou=Computers
# UNIX-Vertrauenskonten-Informationen in LDAP
# (lesen Sie die smb.conf-Manpage fuer mehr Details)
# Angabe der Base-DN, die beim Durchsuchen des Verzeichnisses verwendet wird
        ldap suffix = dc=quenya,dc=org
# Im Allgemeinen ist der Standard-LDAP-Suchfilter OK
        ldap filter = (&(uid=%u)(objectclass=sambaSamAccount))
```

10.10.4.7 Sicherheit und sambaSamAccount

Es gibt zwei wichtige Punkte, an die man sich erinnern sollte, wenn man die Sicherheit von sambaSamAccount-Einträgen im Verzeichnis diskutiert:

- Beziehen Sie *niemals* den Wert von lmPassword- oder ntPassword-Attributen über eine unverschlüsselte LDAP-Sitzung.
- Erlauben Sie *niemals* Nicht-Administrator-Benutzern, die Attributwerte von lmPassword oder ntPassword zu sehen.

Diese Passwort-Hashes sind Klartext-Äquivalente und können dazu verwendet werden, den Benutzer zu verkörpern, ohne die originalen Klartext-Strings zu beziehen. Lesen Sie den Abschnitt Die Account-Datenbank, um mehr Informationen und Details zu LM/NT Passwort-Hashes zu erhalten.

Um die erste Angelegenheit zu bereinigen, ist der voreingestellte Wert für den `smb.conf`-Parameter ldap ssl so, dass eine verschlüsselte Sitzung erforderlich ist (ldap ssl = on), die den Standard-Port `636` verwendet, wenn man den Verzeichnis-Server kontaktiert. Bei Verwendung eines OpenLDAP-Servers ist es möglich, die erweiterte LDAP-Operation StartTLS anstelle von LDAPS zu verwenden. Seien Sie auf jeden Fall davor gewarnt, diese Sicherheitsoption auszuschalten (ldap ssl = off).

Beachten Sie, dass das LDAPS-Protokoll veraltet ist, es wurde durch die erweiterte LDAPv3-Operation StartTLS ersetzt. Die OpenLDAP-Bibliothek bietet jedoch nach wie vor Unterstützung für die ältere Methode zur Absicherung der Client-Server-Kommunikation.

Die zweite Sicherheitsmaßnahme besteht darin, Benutzer ohne Administrator-Rechte davon abzuhalten, Passwort-Hashes aus dem Verzeichnis abzufragen. Dies kann durch folgende ACL in `slapd.conf` erfolgen:

```
## erlaube der "ldap admin dn" Zugriff, aber lehne alle anderen Zugriffe ab
access to attrs=sambaLMPassword,sambaNTPassword
     by dn="cn=Samba Admin,ou=People,dc=quenya,dc=org" write
     by * none
```

10.10.4.8 Spezielle LDAP-Attribute für sambaSamAccounts

Die Objektklasse sambaSamAccount besteht aus den Komponenten, die in den folgenden Tabellen gezeigt werden: Teil A und Teil B.

Der Großteil dieser Parameter wird nur benötigt, wenn Samba als PDC einer Domäne arbeitet (sehen Sie dazu Domänen-Verwaltung). Die folgenden vier Attribute werden nur mit dem sambaSamAccount-Eintrag verspeichert, wenn ihre Werte nicht gleich den Standard-Werten sind:

- sambaHomePath
- sambaLogonScript
- sambaProfilePath
- sambaHomeDrive

Nehmen wir zum Beispiel an, dass MORIA als PDC konfiguriert wurde und dass logon home = \\%L\%u in dessen Datei `smb.conf` definiert wurde. Wenn ein Benutzer namens „*becky*“ sich an der Domäne anmeldet, wird der String logon home auf \\MORIA\becky erweitert. Wenn das Attribut smbHome im Eintrag „*uid=becky,ou=People,dc=samba,dc=org*“ existiert, wird dessen Wert verwendet. Existiert dieses Attribut nicht, wird stattdessen der Wert des Parameters logon home verwendet. Samba schreibt den Attributwert nur dann in den Verzeichniseintrag, wenn der Wert vom Standardwert abweicht (z.B. `\\MOBY\becky`).

10.10.4.9 Beispiel für LDIF-Einträge eines sambaSamAccount

Das folgende Beispiel ist ein funktionierendes LDIF, das die Verwendung der SambaSamAccount-Objektklasse zeigt:

```
dn: uid=guest2, ou=People,dc=quenya,dc=org
sambaLMPassword: 878D8014606CDA29677A44EFA1353FC7
sambaPwdMustChange: 2147483647
sambaPrimaryGroupSID: S-1-5-21-2447931902-1787058256-3961074038-513
sambaNTPassword: 552902031BEDE9EFAAD3B435B51404EE
sambaPwdLastSet: 1010179124
sambaLogonTime: 0
objectClass: sambaSamAccount
uid: guest2
sambaKickoffTime: 2147483647
sambaAcctFlags: [UX         ]
sambaLogoffTime: 2147483647
sambaSID: S-1-5-21-2447931902-1787058256-3961074038-5006
sambaPwdCanChange: 0
```

Hier sehen Sie einen LDIF-Eintrag zur gemeinsamen Verwendung der Objektklassen sambaSamAccount und posixAccount:

```
dn: uid=gcarter, ou=People,dc=quenya,dc=org
sambaLogonTime: 0
displayName: Gerald Carter
sambaLMPassword: 552902031BEDE9EFAAD3B435B51404EE
sambaPrimaryGroupSID: S-1-5-21-2447931902-1787058256-3961074038-1201
objectClass: posixAccount
objectClass: sambaSamAccount
sambaAcctFlags: [UX         ]
userPassword: {crypt}BpM2ej8Rkzogo
uid: gcarter
uidNumber: 9000
cn: Gerald Carter
loginShell: /bin/bash
logoffTime: 2147483647
gidNumber: 100
sambaKickoffTime: 2147483647
sambaPwdLastSet: 1010179230
sambaSID: S-1-5-21-2447931902-1787058256-3961074038-5004
homeDirectory: /home/moria/gcarter
sambaPwdCanChange: 0
sambaPwdMustChange: 2147483647
sambaNTPassword: 878D8014606CDA29677A44EFA1353FC7
```

10.10.4.10 Die Synchronisation von Passwörtern

Samba-3 und spätere Versionen können das Nicht-Samba-(LDAP-)Passwort ändern, das für ein Konto gespeichert wurde. Bei der Verwendung von pam_ldap erlaubt dies das

gleichzeitige Ändern von UNIX- und Windows-Passwörtern.

Die Option ldap passwd sync kann die in der nächsten Tabelle gezeigten Werte annehmen.

Mehr Informationen dazu finden Sie in der Manpage zu `smb.conf`.

10.10.5 MySQL

Immer wieder kommt jemand mit einer großartigen neuen Idee daher. Das Speichern von Benutzerkonten in einem SQL-Backend ist eine solche. Jene, die dies tun wollen, werden wohl am besten beurteilen können, welche spezifischen Vorteile dies für sie hat. Dies klingt wohl nach Rückzug, aber tatsächlich können wir hier nicht versuchen, jedes kleine Detail zu dokumentieren und zu zeigen, warum bestimmte Dinge, die von marginalem Nutzen für das Gros der Samba-Benutzer sind, für den Rest sehr wohl Sinn machen können. In jedem Fall sollten die folgenden Anweisungen dem willigen SQL-Anwender dabei helfen, ein funktionierendes System zu implementieren.

10.10.5.1 Das Anlegen der Datenbank

Sie können Ihre eigene Tabelle anlegen und deren Feldnamen für pdb_mysql angeben (sehen Sie weiter unten nach den Spaltennamen) oder die Standard-Tabelle verwenden. Die Datei `examples/pdb/mysql/mysql.dump` enthält die korrekten Abfragen, um die erforderlichen Tabellen anzulegen. Verwenden Sie den Befehl:

```
$ mysql -uusername -hhostname -ppassword \
   databasename < /path/to/samba/examples/pdb/mysql/mysql.dump
```

10.10.5.2 Konfigurieren

Diesem Plugin fehlt eine gute Dokumentation, aber hier ist etwas Kurz-Information. Fügen Sie Folgendes der Variable passdb backend in Ihrer `smb.conf` hinzu: *passdb backend = [ander*

Der Identifier kann jeder beliebige String sein, solange er nicht mit den Identifiern anderer Plugins oder denen anderer pdb_mysql-Instanzen kollidiert. Wenn Sie mehrere pdb_mysql.so Einträge in passdb backend angeben, müssen Sie auch verschiedene Identifier angeben.

Zusätzliche Optionen können im Abschnitt *[global]* der Datei `smb.conf` angegeben werden. Sehen Sie sich die folgende Tabelle an.

WARNUNG

Da das Passwort des MySQL-Benutzers in der Datei `smb.conf` abgelegt wird, sollten Sie diese Datei nur für den Benutzer lesbar machen, der Samba ausführt. Dies wird als Sicherheitslücke betrachtet und wird bald bereinigt werden.

Die Spaltenbezeichnungen werden in der nächsten Tabelle angegeben. Die Standard-Spaltenbezeichnungen können dem Beispieltabellen-Dump entnommen werden.

Sie können einen Doppelpunkt (:) nach dem Namen jeder Spalte angeben, der ein Update der Spalte beim Update der Tabelle auslöst. Sie können auch nichts nach dem Spaltennamen angeben; dann werden die Felddaten nicht aktualisiert. Das Setzen eines Spaltennamens auf *NULL* bedeutet, dass dieses Feld nicht verwendet werden soll.

Eine Beispielkonfiguration sieht so aus:

Beispiel 10.10.2. Beispielkonfiguration für das MySQL-passdb-Backend

```
[global]
        passdb backend = mysql:foo
        foo:mysql user = samba
        foo:mysql password = abmas
        foo:mysql database = samba
# Der Domänen-Name ist statisch und kann nicht geändert werden
        foo:domain column = 'MYWORKGROUP':
# Der vollständige Name besteht aus den Werten einiger anderer Spalten
        foo:fullname column = CONCAT(firstname,' ',surname):
# Samba sollte niemals in die Passwort-Spalten schreiben
        foo:lanman pass column = lm_pass:
        foo:nt pass column = nt_pass:
# Die Spalte „unknown 3 column“ wird nicht gespeichert
        foo:unknown 3 column = NULL
```

10.10.5.3 Klartext-Passwörter oder verschlüsselte Passwörter

Ich rate entschieden von der Verwendung von Klartext-Passwörtern ab; Sie können diese jedoch verwenden.

Wenn Sie Klartext-Passwörter verwenden wollen, setzen Sie 'identifier:lanman pass column' und 'identifier:nt pass column' auf 'NULL' (ohne die Hochkommas) und 'identifier:plain pass column' auf den Namen der Spalte, die die Klartext-Passwörter enthält.

Wenn Sie verschlüsselte Passwörter verwenden, setzen Sie 'identifier:plain pass column' auf 'NULL' (ohne die Hochkommas). Dies ist die Voreinstellung.

10.10.5.4 Das Beziehen von Nicht-Spalten-Daten aus der Tabelle

Es ist möglich, durch Verwendung einer 'Konstanten' nicht alle Daten in der Datenbank zu halten.

Zum Beispiel können Sie 'identifier:fullname column' auf etwas wie **CONCAT(Firstname,' ',Surname)** setzen.

Oder 'identifier:workstations column' auf: **NULL**

Lesen Sie die MySQL-Dokumentation für mehr Informationen zu den Sprachkonstrukten.

10.10.6 XML

Dieses Modul setzt voraus, dass libxml2 installiert ist.

Die Verwendung von pdb_xml ist ziemlich einfach. Um Daten zu exportieren, verwenden Sie:

```
$ pdbedit -e xml:dateiname
```

(wobei dateiname der Name der Ausgabedatei ist)

Um Daten zu importieren, verwenden Sie: `$ pdbedit -i xml:dateiname`

10.11 Gängige Fehler

10.11.1 Benutzer können sich nicht anmelden

„*Ich habe Samba installiert, aber jetzt kann ich mich mit meinem UNIX-Konto nicht anmelden!*“

Stellen Sie sicher, dass Ihr Benutzer zum aktuellen Samba-passdb-Backend hinzugefügt wurde. Lesen Sie dazu den Abschnitt Werkzeuge zur Verwaltung von Konten.

10.11.2 Benutzer werden zur falschen Backend-Datenbank hinzugefügt

Wir haben ein paar Beschwerden von Benutzern erhalten, die gerade zu Samba-3 gewechselt waren. Die folgenden Einträge in `smb.conf` verursachten Probleme: Neue Konten wurden zur alten smbpasswd-Datei hinzugefügt, nicht zur tdbsam-Datei passdb.tdb:

```
[global]
...
        passdb backend = smbpasswd, tdbsam
...
```

Samba fügt neue Konten zum ersten Eintrag im Parameter *passdb backend* hinzu. Wenn Sie Updates gegen die tdbsam haben wollen, ändern Sie den Eintrag auf:

```
        passdb backend = tdbsam, smbpasswd
```

10.11.3 Konfiguration der auth methods

Beim expliziten Setzen des Parameters auth methods, muss *guest* als der erste Eintrag auf dieser Zeile angegeben werden, z.B. auth methods = guest sam.

Dies ist das exakte Gegenteil zur Anforderung der Option passdb backend, wo *guest* der *LETZTE* Parameter der Zeile sein muss.

Tabelle 10.5. Attribute in der sambaSamAccount-Objektklasse (LDAP) — Teil A

`sambaLMPassword`	Der LANMAN-Passwort-16-Byte-Hash, gespeichert als char-Darstellung eines Hexadezimal-Strings
`sambaNTPassword`	Der NT-Passwort-16-Byte-Hash, gespeichert als char-Darstellung eines Hexadezimal-Strings
`sambaPwdLastSet`	Die integer-Zeit (angegeben in Sekunden seit 1970), die vergangen ist, seitdem die Attribute `sambaLMPassword` und `sambaNTPassword` zuletzt gesetzt wurden.
`sambaAcctFlags`	String mit 11 Zeichen Länge, eingeschlossen von eckigen Klammern []. Er stellt Konto-Flags dar, wie U (user), W (workstation), X (kein Ablauf von Passwörtern), I (Domänen-Vertrauenskonto), H (Heimatverzeichnis erforderlich), S (Server-Vertrauenskonto) und D (disabled).
`sambaLogonTime`	Integer-Wert, derzeit unbenutzt
`sambaLogoffTime`	Integer-Wert, derzeit unbenutzt
`sambaKickoffTime`	Angabe der Zeit (UNIX-Zeitformat), nach der der Benutzer gesperrt wird und sich nicht mehr anmelden kann. Wenn dieses Attribut nicht angegeben wird, läuft das Konto nie ab. Wenn Sie dieses Attribut gemeinsam mit dem Attribut 'shadowExpire' der Objektklasse 'shadowAccount' verwenden, wird dies ermöglichen, Konten zu einem definierten Zeitpunkt komplett ablaufen zu lassen.
`sambaPwdCanChange`	Angabe der Zeit (UNIX-Zeitformat), nach der dem Benutzer erlaubt wird, sein Passwort zu ändern. Wenn dieses Attribut nicht angegeben wird, steht es dem Benutzer frei, sein Passwort zu ändern, wann immer er möchte.
`sambaPwdMustChange`	Angabe der Zeit (UNIX-Zeitformat), ab der der Benutzer gezwungen wird, sein Passwort zu ändern. Wenn dieses Attribut auf '0' gesetzt wird, muss der Benutzer sein Passwort bei der ersten Anmeldung ändern. Wenn dieses Attribut nicht gesetzt wird, läuft das Passwort nie ab.
`sambaHomeDrive`	Angabe des Laufwerksbuchstabens, der auf den UNC-Pfad zeigt, der in sambaHomePath angegeben wurde. Der Laufwerksbuchstabe muss in der Form „*X:*“ angegeben werden, wobei X der Buchstabe des zugewiesenen Laufwerks ist. Sehen Sie sich den Abschnitt zum Parameter logon drive in der Manpage zu `smb.conf` für mehr Informationen dazu an.
`sambaLogonScript`	Der Wert von sambaLogonScript gibt den Pfad des Anmeldeskripts des Benutzers an, in einer .CMD-, .EXE- oder .BAT-Datei. Dieser String kann auch null sein. Der Pfad ist relativ zur netlogon-Freigabe. Sehen Sie sich den Abschnitt zum Parameter logon script in der Manpage zu `smb.conf` an, um mehr Details dazu zu erfahren.
`sambaProfilePath`	Angabe des Pfads zum Profil des Benutzers. Dieser Wert kann auch ein Leerstring sein, ein lokaler absoluter Pfad oder ein UNC-Pfad. Sehen Sie sich den Abschnitt zum Parameter logon path in der Manpage zu `smb.conf` an, um mehr Details dazu zu erfahren.
`sambaHomePath`	Der Wert von sambaHomePath gibt den Pfad des Heimatverzeichnisses des Benutzers an. Dieser Wert kann auch ein Leerstring sein. Wenn sambaHomeDrive gesetzt ist und einen Lauf-

Tabelle 10.6. Attribute in der sambaSamAccount-Objektklasse (LDAP) — Teil B

`sambaUserWorkstations`	Hier können Sie eine komma-getrennte Liste von Maschinen angeben, an denen sich der Benutzer anmelden darf. Es könnten Probleme auftreten, wenn Sie sich an einem Samba-Domänen-Mitglied anzumelden versuchen. Weil Domänen-Mitglieder nicht in dieser Liste sind, werden die Domänencontroller sie zurückweisen. Wo dieses Attribut weggelassen wird, setzt die Standard-Einstellung keinerlei Einschränkungen.
`sambaSID`	Der Security Identifier (SID) des Benutzers. Die Windows-Entsprechung zu UNIX-UIDs.
`sambaPrimaryGroupSID`	Der Security Identifier (SID) der primären Gruppe des Benutzers.
`sambaDomainName`	Die Domäne, der der Benutzer angehört.

Tabelle 10.7. Mögliche Werte für *ldap passwd sync*

Wert	**Beschreibung**
yes	Wenn der Benutzer sein Passwort ändert, werden die Felder `ntPassword`, `lmPassword` und `password` aktualisiert.
no	Nur `ntPassword` und `lmPassword` werden aktualisiert.
only	Aktualisiere nur das LDAP-Passwort, und überlasse die anderen Felder dem LDAP-Server. Diese Option ist nur mit manchen LDAP-Servern verfügbar, und zwar nur dann, wenn der LDAP-Server LDAP_EXOP_X_MODIFY_PASSWD unterstützt.

Tabelle 10.8. Grundlegende smb.conf-Optionen für das MySQL-passdb-Backend

Feld	**Inhalt**
mysql host	Hostname, Standardwert 'localhost'
mysql password	
mysql user	Standardwert 'samba'
mysql database	Standardwert 'samba'
mysql port	Standardwert 3306
table	Tabelle, die die Benutzer enthält

Tabelle 10.9. MySQL-Feldnamen für das MySQL-passdb-Backend

Feld	Typ	Inhalt
logon time column	int(9)	UNIX-Zeitstempel der letzten Anmeldung des Benutzers
logoff time column	int(9)	UNIX-Zeitstempel der letzten Abmeldung des Benutzers
kickoff time column	int(9)	UNIX-Zeitstempel des Zeitpunkts, zu dem der Benutzer von der Workstation „*hinausgeworfen*“ werden soll (nicht erzwungen)
pass last set time column	int(9)	UNIX-Zeitstempel des Zeitpunkts, zu dem das Passwort zuletzt gesetzt wurde
pass can change time column	int(9)	UNIX-Zeitstempel des Zeitpunkts, ab dem das Passwort geändert werden kann
pass must change time column	int(9)	UNIX-Zeitstempel des Zeitpunkts, ab dem das Passwort geändert werden muss
username column	varchar(255)	UNIX-Benutzername
domain column	varchar(255)	NT-Domäne, der der Benutzer angehört
nt username column	varchar(255)	NT-Benutzername
fullname column	varchar(255)	Vollständiger Name des Benutzers
home dir column	varchar(255)	Pfad des UNIX-Heimatverzeichnisses (äquivalent zum Parameter logon home).
dir drive column	varchar(2)	Laufwerksbuchstabe des Verzeichnisses (z.B. „*H:*“)
logon script column	varchar(255)	Batch-Datei, die bei der Anmeldung ausgeführt werden soll
profile path column	varchar(255)	Pfad zum Profil
acct desc column	varchar(255)	Einige ASCII-NT-Benutzerdaten
workstations column	varchar(255)	Workstations, an denen sich der Benutzer anmelden darf (oder NULL für alle)
unknown string column	varchar(255)	Unbekannter String
munged dial column	varchar(255)	Unbekannt
user sid column	varchar(255)	NT-Benutzer-SID
group sid column	varchar(255)	NT-Gruppen-SID
lanman pass column	varchar(255)	Verschlüsseltes Lanman-Passwort
nt pass column	varchar(255)	Verschlüsseltes NT-Passwort
plain pass column	varchar(255)	Klartext-Passwort
acct ctrl column	int(9)	NT-Benutzerdaten
unknown 3 column	int(9)	Unbekannt
logon divs column	int(9)	Unbekannt
hours len column	int(9)	Unbekannt
bad password count column	int(5)	Anzahl von erlaubten Fehleingaben des Passworts, bevor das Konto deaktiviert wird
logon count column	int(5)	Anzahl von Anmeldeversuchen
unknown 6 column	int(9)	Unbekannt

Kapitel 11

DAS GRUPPEN-MAPPING — ZWISCHEN MS WINDOWS UND UNIX

Mit der Einführung von Samba 3 wurden neue Gruppen-Mapping-Funktionen eingebaut, die Verbindungen zwischen Unix-Gruppen und Windows-Gruppen-SIDs ermöglichen. Das Unterkommando **groupmap**, das zum Kommando net gehört, wird für das Verbinden der Gruppen verwendet.

Die neuen Merkmale des Gruppen-Mappings ermöglichen es dem Administrator zu entscheiden, welche NT-Domänengruppen dem MS Windows-Client zugeordnet werden. Es werden nur jene NT-Domänengruppen in den Werkzeugen zur Bearbeitung von Domänen-Benutzern und -Gruppen angezeigt, die auf eine Unix-Gruppe gemappt wurden und nicht dem Standardwert (`-1`) zugeordnet wurden.

> WARNUNG
>
> Der Parameter *domain admin group* wurde aus Samba-3 entfernt und sollte nicht länger verwendet werden. In Samba-2.2.x-Versionen wurde dieser Parameter verwendet, um einer bestimmten Liste von Benutzern die Mitgliedschaft in der Domänen-Administratoren-Gruppe zu geben, die lokale Administrator- Rechte auf den Client Rechner vergibt (in Standard-Konfigurationen).

11.1 Eigenschaften und Vorzüge

Samba ermöglicht dem Administrator das Anlegen von MS Windows NT4/200x-Gruppenkonten, die auf beliebige UNIX/Linux-Gruppen gemappt werden können.

Gruppenkonten können mit den MS Windows 200x/XP Professional MMC-Tools verwaltet werden. In der Datei `smb.conf` können entsprechende Skripten verwendet werden, um mit diesen MMC-Tools automatisch UNIX/Linux-Konten anzulegen. Wenn diese Skripten nicht angegeben werden und der **winbindd** läuft, werden die Samba-Gruppenkonten den Parametern von idmap uid/idmap gid der `smb.conf` zugeordnet.

Figure 11.1. IDMAP: Auflösung der Gruppen-SID in eine GID

Figure 11.2. IDMAP: GID-Auflösung in eine passende SID

In beiden Fällen können, wenn winbindd nicht läuft, nur lokal auflösbare Gruppen erkannt werden (siehe auch IDMAP: Auflösung der Gruppen SID zur GID und IDMAP: GID Auflösung zu passender SID). Das Kommando **net groupmap** wird verwendet, um UNIX-Gruppen zu NT-SID-Mappings wie in IDMAP: Speichern von Gruppen-Mappings zu erstellen.

Figure 11.3. IDMAP: Speichern von Gruppen-Mappings

Administratoren sollten beachten, dass `smb.conf` Gruppen-Interface-Skripten direkt die UNIX/Linux-Systemwerkzeuge (die Shadow-Utilities **groupadd**, **groupdel** und **groupmod**) verwenden. Die resultierenden Gruppennamen können nur Zeichen enthalten, die auch die oben genannten Werkzeuge bearbeiten können. Wenn die Werkzeuge keine Großbuchstaben oder Leerzeichen erlauben, wird das Erstellen der Gruppe *Domänen-Administratoren* nicht möglich sein.

Es gibt verschiedene Lösungswege für solche Einschränkungen verschiedener Betriebsysteme. Eine Möglichkeit besteht darin, Skripten zu verwenden, die die Systemeinschränkungen kennen und dann nur die UNIX/Linux-Gruppen-ID (GID) an Samba zurückgeben. Dies ist ein dynamischer Workaround.

Ein anderer Lösungsansatz ist die manuelle Erstellung der UNIX/Linux- und MS Windows NT4/200x-Gruppen am Samba-Server und die Verwendung des Werkzeugs **net groupmap**, um die Gruppen zu „*verbinden*“.

11.2 Diskussion

Bei der Installation von MS Windows NT4/200x auf einem Computer erstellt das Installationsprogramm Benutzer und Gruppen, insbesondere die `Administratoren`-Gruppe. Diese Gruppe erhält die nötigen Rechte, um wichtige Systemaufgaben, wie die Änderung der Zeit und das Beenden von Programmen, auszuführen.

Der Benutzer `Administrator` ist Mitglied der Gruppe `Administratoren`. Dies vererbt die Gruppenrechte der `Administratoren`. Falls ein Benutzer `joe` erzeugt wird, der Mitglied

der Gruppe `Administratoren` ist, so hat `joe` genau diesselben Rechte wie der Benutzer `Administrator`.

Wenn eine MS Windows NT/200x/XP-Maschine zum Domänenmitglied gemacht wird, so wird die Gruppe „*Domänen-Administratoren*“ des PDC zu der lokalen Gruppe `Administratoren` der Arbeitsstation hinzugefügt. Jedes Mitglied der Gruppe `Domänen-Administratoren` vererbt die Rechte der lokalen Gruppe `Administratoren`, wenn diese sich an der Arbeitsstation anmelden.

Die folgenden Schritte beschreiben, wie man Samba-PDC-Benutzer zu Mitgliedern der Gruppe `Domänen-Administratoren` macht.

1. Erzeugen Sie eine UNIX-Gruppe (normalerweise in der Datei `/etc/group`); nennen wir sie `domadm`.

2. Fügen Sie dieser Gruppe die Benutzer hinzu, die „*Administrator*“ sein müssen. Falls Sie zum Beispiel `joe, john` und `mary` Administrator sein lassen wollen, sieht Ihr Eintrag in `/etc/group` wie folgt aus:

   ```
   domadm:x:502:joe,john,mary
   ```

3. Mappen Sie diese domadm-Gruppe auf die Gruppe „*Domänen-Administratoren*“, indem Sie den folgenden Befehl eingeben:

   ```
   root# net groupmap add ntgroup=Domänen Administratoren unixgroup=domadm
   ```

   Die Anführungszeichen um „*Domänen Administratoren*“ sind notwendig, weil der Gruppenname ein Leerzeichen enthält. Stellen Sie zudem sicher, dass Sie keine Leerzeichen um das Gleichheitszeichen (=) übrig lassen.

Jetzt sind `joe, john` und `mary` Domänenadministratoren.

Es ist möglich, jede beliebige UNIX-Gruppe auf jede Windows NT4/200x-Gruppe zu mappen, genauso wie jede UNIX-Gruppe zu einer Windows-Domänengruppe zu machen. Wenn Sie beispielsweise eine UNIX-Gruppe (z.B. acct) in eine ACL auf einer lokalen Datei oder Drucker auf einer Domänen-Mitgliedsmaschine aufnehmen wollen, dann markieren Sie diese Gruppe als eine Domänengruppe auf dem Samba-PDC, indem Sie Folgendes eingeben:

```
root# net groupmap add rid=1000 ntgroup="Accounting" unixgroup=acct
```

Beachten Sie, dass der RID-Parameter ein unsigned 32-Bit-Integer ist, der normalerweise bei 1000 startet. Dieser RID darf sich jedoch nicht mit einem RID überschneiden, der einem Benutzer zugewiesen ist. Dies wird mit unterschiedlichen Verfahren überprüft, die von dem von Ihnen verwendeten passdb-Backend abhängen. Künftige Versionen der Werkzeuge nehmen die Überprüfung eventuell automatisch vor, aber derzeit ist dies Ihre Aufgabe.

11.2.1 Wichtige administrative Informationen

Administrative Rechte sind in zwei spezifischen Formen notwendig:

1. Für Samba-3-Domänencontroller und Domänen-Mitgliedsserver/Clients
2. Um Windows-Arbeitsstationen, die Domänenmitglied sind, zu verwalten

Administrative Aufgaben auf UNIX/Linux-Systemen, wie das Hinzufügen von Benutzern oder Gruppen, setzen `root`-Level-Privilegien voraus. Das Hinzufügen eines Windows-Clients zu einer Samba-Domäne bringt das Hinzufügen eines Benutzerkontos für den Windows-Client mit sich.

Viele UNIX-Administratoren beantragen wiederholt beim Samba-Team, es zu ermöglichen, ohne `root`-Rechte Windows-Arbeitsstationen oder Benutzerkonten hinzuzufügen und zu löschen. Eine solche Anfrage verletzt jedes Verständnis von grundlegender UNIX-Systemsicherheit.

Es gibt keinen sicheren Weg, den Zugriff auf ein UNIX/Linux-System ohne `root`-Privilegien zur Verfügung zu stellen. Die Bereitstellung von `root`-Privilegien kann entweder durch Anmelden als `root` an der Domäne erfolgen, oder man kann bestimmten Benutzern erlauben, ein UNIX-Konto zu benutzen, das Mitglied der UNIX-Gruppe ist, für die GID=0 als primäre Gruppe in der Datenbank `/etc/passwd` definiert ist. Benutzer solcher Konten können Werkzeuge wie den NT 4-Domänen-Benutzermanager und den NT 4-Domänen-Servermanager verwenden, um Benutzer- und Gruppenkonten ebenso zu verwalten wie Domänen-Mitgliedsserver und Client-Konten. Diese Privilegienebene wird ebenfalls benötigt, um ACLs auf Freigabeebene zu verwalten.

Administrative Aufgaben auf einer Windows-Arbeitsstation, die Domänenmitglied ist, können durch jeden, der Mitglied der Gruppe `Domänen Administratoren` ist, durchgeführt werden. Diese Gruppe kann auf jede passende UNIX-Gruppe gemappt werden.

11.2.2 Standardbezeichner für Benutzer, Gruppen und Beziehungen

Beim ersten Installieren wird Microsoft Windows NT4/200x/XP mit einigen Benutzer-, Gruppen- und Alias-Einheiten vorkonfiguriert. Jede hat einen bekannten relativen Bezeichner (RID). Dieser muss für die weitergehende Integrität von Operationen eindeutig bleiben. Samba muss mit gewissen lebensnotwendigen Domänengruppen ausgestattet werden, die den entsprechenden RID-Wert verlangen. Wenn Samba-3 so konfiguriert wird, dass es `tdbsam` nutzt, werden die lebensnotwendigen Domänengruppen automatisch angelegt. Es ist dann die Verantwortung des LDAP-Administrators, die Standard-NT-Gruppen zu erzeugen (diese auszustatten).

Jede grundlegende Domänengruppe muss ihrer zugehörigen bekannten RID zugeordnet werden. Die Standard-Benutzer, Gruppen, Aliases und RIDs werden in der Tabelle Bekannte Standardbenutzer-RIDs angezeigt.

ANMERKUNG

Wenn das *passdb backend* LDAP (`ldapsam`) benutzt, ist der Administrator dafür verantwortlich, die notwendigen Domänengruppen zu erzeugen und diese ihrer jeweiligen RID zuzuweisen.

Es ist zulässig, jede Domänengruppe, die benötigt wird, zu erzeugen. Stellen Sie lediglich sicher, dass die notwendige (bekannt gegebene) Domänengruppe erzeugt worden ist und Ihrer Standard-RID zugewiesen worden ist. Andere Gruppen, die Sie anlegen, können Sie jeder beliebigen RID zuordnen, die Sie benutzen möchten.

Stellen Sie sicher, dass jede Domänengruppe auf eine UNIX-Systemgruppe gemappt wird. Dies ist der einzige Weg, um sicherzustellen, dass die Gruppe als eine NT-Domänengruppe verfügbar sein wird.

Tabelle 11.1. Bekannte Standardbenutzer-RIDs

Bekannte Einheit	RID	Typ	Notwendig
Domänen-Administrator	500	Benutzer	Nein
Domänen-Gast	501	Benutzer	Nein
Domäne KRBTGT	502	Benutzer	Nein
Domänen-Administratoren	512	Gruppe	Ja
Domänenbenutzer	513	Gruppe	Ja
Domänengäste	514	Gruppe	Ja
Domänencomputer	515	Gruppe	Nein
Domänencontroller	516	Gruppe	Nein
Domänen-Certificate-Administratoren	517	Gruppe	Nein
Domänen-Schema-Administratoren	518	Gruppe	Nein
Domänen-Enterprise-Administratoren	519	Gruppe	Nein
Domänen-Policy-Administratoren	520	Gruppe	Nein
Builtin-Administratoren	544	Alias	Nein
Builtin-Benutzer	545	Alias	Nein
Builtin-Gäste	546	Alias	Nein
Builtin-Hauptbenutzer	547	Alias	Nein
Builtin-Zugriffsoperator	548	Alias	Nein
Builtin-System-Operator	549	Alias	Nein
Builtin-Drucker-Operator	550	Alias	Nein
Builtin-Backup-Operator	551	Alias	Nein
Builtin-Replikator	552	Alias	Nein
Builtin-RAS-Server	553	Alias	Nein

11.2.3 Beispielkonfiguration

Sie können die verschiedenen Gruppen in der Mapping-Datenbank anzeigen lassen, indem Sie **net groupmap list** eingeben. Hier ist ein Beispiel:

```
root#  net groupmap list
Domänen Administratoren (S-1-5-21-2547222302-1596225915-2414751004-512) -> domadmin
Domänen Benutzer (S-1-5-21-2547222302-1596225915-2414751004-513) -> domuser
Domänen Gäste (S-1-5-21-2547222302-1596225915-2414751004-514) -> domguest
```

Ausführliche Details zu **net groupmap** finden Sie auf der net(8)-Manpage.

11.3 Konfigurationskripten

Jeder braucht Werkzeuge. Manche von uns erstellen ihre gern selbst, andere bevorzugen Werkzeuge aus der Konserve (z.B. solche, die von jemandem für bestimmte Zwecke vorbereitet wurden).

11.3.1 Beispiel für ein smb.conf-Skript zum Hinzufügen von Gruppen

smbgrpadd.sh ist ein Skript, um übereinstimmende Gruppennamen für die Nutzung durch das Samba-Gruppeninterface zu erstellen.

Beispiel 11.3.1. smbgrpadd.sh

```
#!/bin/bash

# Fügt die Gruppe unter Nutzung des normalen groupadd-Systemwerkzeugs hinzu.
groupadd smbtmpgrp00

thegid=‘cat /etc/group | grep smbtmpgrp00 | cut -d ":" -f3‘

# Jetzt den Namen für unser MS Windows-Netzwerk passend ändern.
cp /etc/group /etc/group.bak
cat /etc/group.bak | sed "s/smbtmpgrp00/$1/g" > /etc/group

# Melde uns die GID zurück.
echo $thegid
exit 0
```

Der `smb.conf`-Eintrag für obiges Skript kann etwas wie in dem folgenden Beispiel sein.

11.3.2 Skript zum Konfigurieren von Gruppen-Mappings

In unserem Beispiel haben wir eine UNIX/Linux-Gruppe namens *ntadmin* erzeugt. Unser Skript wird die zusätzlichen Gruppen *Orks*, *Elfen* und *Gnome* anlegen. Es ist eine gute Idee, dieses Shellskript für eine spätere erneute Nutzung abzuspeichern, auch für den Fall, dass

Beispiel 11.3.2. Konfiguration von smb.conf für das Skript zum Gruppenhinzufügen.

```
[global]
...
        add group script = /Pfad_zum_Werkzeug/smbgrpadd.sh "%g"
...
```

Sie später Ihre Mapping-Datenbank einmal neu anlegen müssen. Aus praktischen Gründen entscheiden wir uns, dieses Skript als eine Datei namens `initGroups.sh` zu speichern. Dieses Skript heißt in diesem Beispiel initGroups.sh.

Beispiel 11.3.3. Skript zum Setzen von Gruppen-Mappings

```
#!/bin/bash

net groupmap modify ntgroup="Domänen Administratoren" unixgroup=ntadmin
net groupmap modify ntgroup="Domänen Benutzer" unixgroup=users
net groupmap modify ntgroup="Domänen Gäste" unixgroup=nobody

groupadd Orks
groupadd Elfen
groupadd Gnome

net groupmap add ntgroup="Orks"   unixgroup=Orks   type=d
net groupmap add ntgroup="Elfen"  unixgroup=Elfen  type=d
net groupmap add ntgroup="Gnome"  unixgroup=Gnome  type=d
```

Natürlich wird vorausgesetzt, dass der Administrator dies für lokale Zwecke anpasst. Für Informationen zur Nutzung des Werkzeugs **net groupmap** sehen Sie bitte in der Manpage nach.

11.4 Gängige Fehler

Zurzeit gibt es eine Menge kleiner Überraschungen für den unachtsamen Administrator. In gewisser Weise ist es erforderlich, dass jeder Schritt automatisierter Kontrollskripten sorgfältig manuell getestet wird, bevor diese in der Praxis verwendet werden.

11.4.1 Das Hinzufügen von Gruppen schlägt fehl

Dies ist ein häufiges Problem, wenn **groupadd** direkt von dem Samba-Interface-Skript für add group script (Parameter in der Datei `smb.conf`) aufgerufen wurde.

Der häufigste Grund für diesen Fehler ist der Versuch, ein MS Windows-Gruppenkonto hinzuzufügen, das entweder ein großgeschriebenes Zeichen und/oder ein Leerzeichen enthält.

Es gibt drei mögliche Workarounds. Erstens: Benutzen Sie nur Gruppennamen, die mit den Einschränkungen des UNIX/Linux-Systemwerkzeugs **groupadd** zurechtkommen. Der zweite betrifft die Benutzung des Skripts, welches weiter oben in diesem Kapitel erwähnt wurde, und der dritte ist die Option, ein UNIX/Linux-Gruppenkonto manuell anzulegen, das zu dem MS Windows-Gruppennamen passt; dann benutzen Sie den oben beschriebenen Ablauf, um diese Gruppe auf eine MS Windows-Gruppe zu mappen.

11.4.2 Das Hinzufügen von MS Windows-Gruppen zu MS Windows-Gruppen schlägt fehl

Samba-3 unterstützt keine verschachtelten Gruppen aus der MS Windows-Kontrollumgebung.

11.4.3 *Domänen Benutzer* zu der Gruppe *Hauptbenutzer* hinzufügen

„*Was muss ich machen, um Domänenbenutzer zu der Hauptbenutzer-Gruppe hinzuzufügen?*“ Die Hauptbenutzer-Gruppe ist eine Gruppe, die lokal auf jeder Windows 200x/XP Professional-Arbeitsstation vorhanden ist. Sie können die Domänen-Benutzergruppe nicht automatisch zu der Hauptbenutzer-Gruppe hinzufügen. Dazu müssen Sie sich auf jeder Arbeitsstation als der lokale Arbeitsstations-*Administrator* und anmelden und folgende Prozedur abarbeiten:

1. Klicken Sie auf **Start** -> **Systemsteuerung** -> **Benutzer und Kennwörter**.
2. Klicken Sie auf die Registerkarte **Erweitert**.
3. Klicken Sie auf den Button **Erweitert**.
4. Klicken Sie auf `Gruppen`.
5. Doppelklicken Sie auf `Hauptbenutzer`. Dies lässt das Feld zum Hinzufügen von Benutzern und Gruppen zu der lokalen Gruppe `Hauptbenutzer` erscheinen.
6. Klicken Sie auf den Button **Hinzufügen**.
7. Wählen Sie die Domäne aus, von der Sie die Gruppe `Domänen Benutzer` hinzufügen.
8. Doppelklicken Sie auf die Gruppe `Domänen Benutzer`.
9. Klicken Sie auf den Button **Ok**. Falls während dieses Prozesses eine Anmeldebox erscheint, denken Sie bitte daran, die Anmeldung als `Domäne\Benutzername` durchzuführen. Für die Domäne `MITTELERDE` und den Benutzer `root` geben Sie beispielsweise `MITTELERDE\root` ein.

Kapitel 12

ZUGRIFFSKONTROLLEN FÜR DATEIEN, VERZEICHNISSE UND NETZWERK-FREIGABEN

Fortgeschrittene Windows-Benutzer sind häufig verwirrt, wenn sich eine Änderung der Besitzrexhte an Dateien oder Verzeichnissen auf dem Samba-Server nicht so auswirkt, wie sie es erwarten. MS-Administratoren verwirrt es oft, wenn sie versuchen, Ihre Daten mit Zugriffskontroll-Listen vor unerlaubten Zugriffen zu schützen.

Viele UNIX-Administratoren sind nicht mit der MS Windows-Umgebung vertraut. Besondere Probleme ergeben sich aus den Benutzerwünschen bezüglich der Kontrolle von Dateien und Verzeichnissen und deren Einrichtung.

Das Problem rührt aus den Unterschieden bei den Datei- und Verzeichnis-Benutzerrechten der beiden Systeme her. Diesen Unterschied kann auch Samba nicht wirklich aus der Welt schaffen, aber es schafft eine Brücke zwischen den Umgebungen.

Die POSIX-(UNIX, LINUX-)Zugriffskontroll-Technologie (ACLs) gibt es schon seit Jahren, aber sie wurde nie sehr intensiv genutzt. Dies erklärt vielleicht auch, warum es so lange gedauert hat, bis die die ACL-Technik in kommerzielle Linux-Produkte eingebunden wurde. MS-Administratoren wird dies erstaunen, da diese Technik seit Jahren elementarer Bestandteil von Windows-Produkten ist.

Dieses Kapitel soll die Punkte im Einzelnen klären, die mit Samba-3 nötig und möglich sind, damit Administratoren eine optimale Zugriffsverwaltung für ihre Windows-Benutzer einrichten können.

Samba ist nicht primär dafür gedacht, eine Unix-Plattform in eine Windows-Plattform zu verwandeln, sondern soll die bestmögliche Kompatibilität zwischen den beiden Systemen schaffen.

12.1 Möglichkeiten und Vorteile

Samba ermöglicht eine hohe Flexibilität beim Systemzugriff. Hier sind es die Zugriffskontrollmöglichkeiten der aktuellen Version 3 von Samba.

Samba-Zugriffskontrollmöglichkeiten

- *Unix-Datei- und -Verzeichnis-Berechtigungen*

  Samba arbeitet mit den UNIX-Dateizugriffskontrollen zusammen. Benutzer greifen dabei als Windows-Benutzer auf Samba zu. Informationen über den Benutzer werden beim Einloggen übergeben. Samba benutzt diese Login-Informationen, um zu entscheiden, ob einem Benutzer Zugriff auf Systemdaten gewährt werden soll oder nicht. Dieses Kapitel enthält eine Übersicht über UNIX-Berechtigungen für Nutzer, die diese nicht kennen oder diese für etwas verwirrend halten.

- *Samba-Netzlaufwerksdefinitionen*

  Beim Konfigurieren von Netzlaufwerken mit Samba in der Datei smb.conf kann der Administrator Berechtigungen des darunter liegenden Dateisystems verändern und beeinflussen. Dies ermöglicht teilweise eine Annäherung an das Verhalten, das Windows-Benutzer erwarten. Dieser Weg ist aber nur selten die beste Lösung. Die grundlegenden Möglichkeiten werden hier beschrieben.

- *Samba-Netzlaufwerkskontroll-Listen*

  Wie in Windows NT ist es auch in Samba möglich, Netzlaufwerkskontroll-Listen zu erstellen. Einige Anwender machen Gebrauch davon. Es ist zurzeit eine der leichtesten Möglichkeiten, Zugriffskontrolle zu erreichen, im Gegensatz zu anderen komplexeren Methoden.

- *MS Windows-Zugriffskontroll-Listen und UNIX-Zugriffskontroll-Listen*

  Der Gebrauch von UNIX-Kontroll-Listen ist nur möglich, wenn diese Funktionen in dem darunter liegenden Dateisystem implementiert sind. In jedem anderen Fall ist deren Nutzung nicht möglich. Aktuelle Unix-Systeme sollten diese Unterstützung bieten. Es gibt Patches für den Linux-Kernel, die diese Möglichkeit implementieren, falls sie noch nicht vorhanden ist. Viele Unix-Systeme werden mit der Unterstützung ausgeliefert, und in diesem Kapitel versuchen wir, den Benutzern deren Gebrauch zu erklären.

12.2 Die Zugriffskontrollen des Dateisystems

Es ist wichtig festzustellen, dass MS Windows ein völlig anderes Dateizugriffssystem benutzt als UNIX-Systeme. Wir werden erst die Unterschiede erklären und dann zeigen, wie Samba hilft, diese Unterschiede zu überbrücken.

12.2.1 Vergleich zwischen NTFS und dem UNIX-Dateisystem

Samba benutzt das UNIX-Dateisystem, d.h., Samba verhält sich innerhalb der Möglichkeiten des UNIX-Dateisystems. Aber Samba ist auch dafür verantwortlich, das Verhalten des Windows-Dateisystems nachzustellen.

Glücklicherweise bietet Samba eine Reihe von Konfigurationsmöglichkeiten, um die Unterschiede zu überbrücken. Wir werden einige dieser Einstellungsmöglichkeiten betrachten, jedoch nicht alle. Wer mehr wissen möchte, sollte die Manpage der Datei smb.conf lesen.

Im Folgenden sehen Sie einen Vergleich des UNIX-Dateisystems mit dem Dateisystem von Windows NT/200x:

Namensraum Windows-Dateinamen können 254 Zeichen lang sein, UNIX beherrscht bis zu 1023 Zeichen. Die Dateierweiterung beschreibt in Windows einen bestimmten Dateityp, in UNIX-Systemen ist das nicht zwingend so.

Was unter Windows ein 'Ordner' ist, heißt in UNIX 'Verzeichnis'.

Groß-/Kleinschreibung Im Allgemeinen sind Dateinamen unter Windows 8+3 Zeichen lang und werden in Großbuchstaben erstellt. Dateinamen, die länger sind, sind in ihrer Schreibweise case-insensitive (d.h., es spielt keine Rolle, ob sie groß- oder kleingeschrieben werden).

Unter UNIX sind alle Dateien und Verzeichnisse case-sensitive (d.h., es spielt sehr wohl eine Rolle, ob ein Dateiname groß- oder kleingeschrieben wird).

Im folgenden Beispiel würden die Dateinamen von Windows völlig gleich interpretiert werden, für UNIX wären es drei verschiedene Dateien:

```
MYFILE.TXT
MyFile.txt
myfile.txt
```

Es wird ziemlich klar, dass diese Dateien in Windows nicht nebeneinander (im selben Ordner) stehen könnten, unter ist das UNIX jedoch jederzeit möglich.

Was soll nun Samba tun, wenn es auf diese Dateien trifft? Die Lösung besteht darin, dass die erste Datei für Windows-Benutzer sichtbar ist, die anderen jedoch nicht verfügbar bzw. unsichtbar sind; eine andere Lösung ist nicht denkbar.

Verzeichnis-Trennzeichen MS Windows und DOS benutzen das Zeichen \ (Backslash) als Verzeichnis-Trennzeichen, UNIX benutzt (wie im Internet üblich) den Slash `/` als Verzeichnis-Trennzeichen. Dies wird von Samba transparent (für den Windows-Benutzer unbemerkt) umgesetzt.

Laufwerksbezeichnung In MS Windows werden verschiedene Festplatten-Partitionen mit Buchstaben belegt. **C:** Es gibt unter UNIX kein ähnliches Konzept, Festplatten-Teile (Partitionen) werden als Teil des Dateisystems eingebunden (gemountet). Was unter DOS `C:\` ist, wäre unter UNIX einfach `/` (root = Wurzel des Dateisystembaums).

Dateinamenskonvention MS Windows kennt keine Dateien, deren Namen mit einem Punkt beginnen (`.`). In UNIX werden solche Dateien häufig in den „*Home*"-Verzeichnissen (Heimatverzeichnissen) von Benutzern gefunden. Punktdateien(`.`) sind typischerweise Start- oder Konfigurationsdateien für UNIX-Programme.

Verknüpfungen und Verkürzungen Unter Windows sind Verknüpfungen spezielle Dateitypen, die zum verkürzten Starten von Programmen in deren realen Ordner dienen. Auch unter UNIX gibt es Verknüpfungen und Verkürzungen, diese werden jedoch völlig unterschiedlich gehandhabt.

Symbolische Verknüpfungen unter UNIX halten die aktuellen Informationen von Dateien oder Verzeichnissen. Schreib- und Lesezugriffe auf eine Verknüpfung verhalten sich genauso wie bei der originalen Datei. Symbolische Verknüpfungen nennt man auch weiche Verknüpfungen. Harte Verknüpfungen kennt MS Windows nicht, diese würden das Benutzen ein- und derselben Datei unter mehreren Namen gleichzeitig ermöglichen.

Es gibt noch viele Unterschiede, die einem Windows-Administrator unangenehm im Umgang mit UNIX sein könnten.

12.2.2 Verwaltung von Verzeichnissen

Es gibt grundsätzlich drei Möglichkeiten, um Ordner (Verzeichnisse) zu verwalten: **create (erstellen)**, **delete (löschen)** und **rename (umbenennen)**.

Tabelle 12.1. Verwaltung von Ordnern (Verzeichnissen) mit UNIX und Windows

Aktion	Windows-Befehl	UNIX-Befehl
create	md folder	mkdir folder
delete	rd folder	rmdir folder
rename	rename oldname newname	mv oldname newname

12.2.3 Die Verwaltung der Zugriffskontrollen von Dateien und Ordnern (Verzeichnissen)

Jedem Administrator wird geraten, zusätzlich Handbücher zu diesem Thema zu studieren. Die meisten Fälle können mit den grundlegenden Zugriffsmöglichkeiten von UNIX gelöst werden, ohne die Technologien der Zugriffskontroll-Listen (ACLs) oder der erweiterten Attribute (EAs) zu verwenden.

Die Datei- und Verzeichnisverwaltung von UNIX basiert auf den folgenden Zugriffsmöglichkeiten:

```
$ ls -la
total 632
drwxr-xr-x   13 maryo   gnomes      816 2003-05-12 22:56 .
drwxrwxr-x   37 maryo   gnomes     3800 2003-05-12 22:29 ..
dr-xr-xr-x    2 maryo   gnomes       48 2003-05-12 22:29 muchado02
drwxrwxrwx    2 maryo   gnomes       48 2003-05-12 22:29 muchado03
drw-rw-rw-    2 maryo   gnomes       48 2003-05-12 22:29 muchado04
d-w--w--w-    2 maryo   gnomes       48 2003-05-12 22:29 muchado05
dr--r--r--    2 maryo   gnomes       48 2003-05-12 22:29 muchado06
drwsrwsrwx    2 maryo   gnomes       48 2003-05-12 22:29 muchado08
```

```
----------    1 maryo    gnomes     1242 2003-05-12 22:31 mydata00.lst
--w--w--w-    1 maryo    gnomes     7754 2003-05-12 22:33 mydata02.lst
-r--r--r--    1 maryo    gnomes    21017 2003-05-12 22:32 mydata04.lst
-rw-rw-rw-    1 maryo    gnomes    41105 2003-05-12 22:32 mydata06.lst
$
```

Die Reihen oben repräsentieren (von rechts nach links): die Berechtigung, die Anzahl der „*harten*“ Links einer Datei, den Besitzer (einer Datei), die Besitzergruppe und die Größe in Bytes.

In Abbildung **??** finden Sie eine Übersicht.

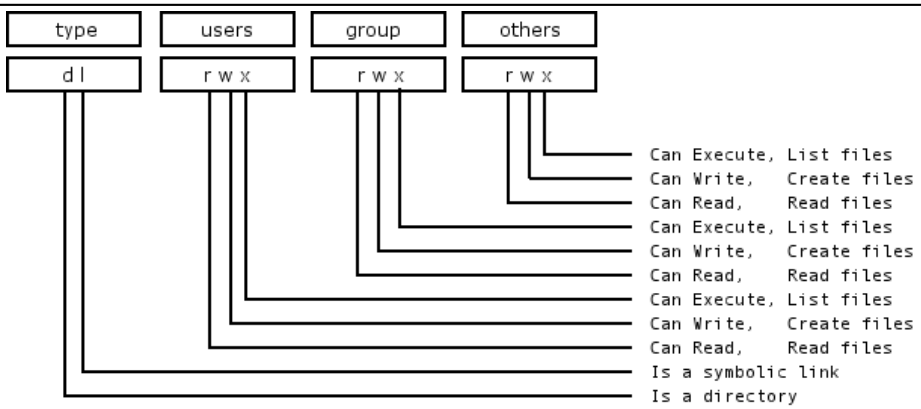


Figure 12.1. Übersicht über die UNIX-Berechtigungen

Jedes Bit kann auch unbesetzt sein und wird durch ein Minus (-) dargestellt.

Beispiel 12.2.1. Beispieldatei

```
-rwxr-x---   Bedeutet: Der Besitzer kann lesen, schreiben und ausführen.
                       Die Gruppe kann lesen und ausführen.
                       Andere haben keine Rechte.
```

Zusätzliche Möglichkeiten im Typen-Feld [type] sind: c = character device, b = block device, p = pipe device, s = UNIX-Domain-Socket.

Die Zeichen `rwxXst` für die Berechtigungen für Nutzer, Gruppen und andere sind: lesen (r), schreiben (w), ausführen (oder Ordner-Zugriff) (x), exklusives Ausführen, wenn der Nutzer berechtigt für die Datei oder den Ordner ist (X), Setzen der ID des Nutzers bei Ausführung (s), Sticky-Bit (begleitendes Bit)(t).

Wenn das Sticky-Bit auf einem Verzeichnis gesetzt ist, können darin enthaltene Dateien nur vom Nutzer root oder dem Ersteller der Dateien gelöscht werden. In jedem anderem Fall sind alle anderen Dateivorgänge (löschen, lesen, umbenennen) erlaubt. Das Sticky-Bit

wird häufig für Verzeichnisse wie das /tmp-Verzeichnis benutzt, die gewöhnlich für jeden beschreibbar sind.

Wenn auf einem Verzeichnis das Gruppen- oder Nutzer-Identitätsbit gesetzt ist, dann erhalten Nutzer und Gruppen Berechtigungen auf darin enthaltene Dateien. Dies ermöglicht das Erstellen von Verzeichnissen, in denen alle Nutzer einer Gruppe auf eine Datei zugreifen können sollen, insbesondere dann, wenn es nicht erwünscht ist, dass diese Datei exklusiv einem Benutzer gehört, der zu einer anderen primären Gruppe gehört als die übrigen Nutzer.

Falls ein Verzeichnis auf `drw-r-----` gesetzt ist, heißt dies, dass der Eigner in ihm Dateien lesen und schreiben (erstellen) kann, aber dadurch, dass das Ausführen-Flag (x) nicht gesetzt ist, können die Dateien in diesem Verzeichnis von niemandem gesehen werden. Die Gruppe kann Dateien lesen, aber keine neuen anlegen. Falls Dateien in dem Verzeichnis für die Gruppe les- oder schreibbar gesetzt sind, können die Gruppenmitglieder diese schreiben oder löschen.

12.3 Zugriffskontrollen für Freigabedefinitionen

Die folgenden Parameter in den Dateisektionen von `smb.conf` definieren eine Freigabekontrolle oder betreffen Zugriffskontrollen. Bevor Sie eine dieser folgenden Optionen benutzen, sehen Sie bitte in den Manpages für `smb.conf` nach.

12.3.1 Benutzer- und gruppen-basierende Kontrollen

Benutzer- und gruppen-basierende Kontrollen können sehr hilfreich sein. In manchen Situationen ist es sogar gewünscht, dass alle Dateisystem-Operationen behandelt werden, als wären sie von einem einzelnen Benutzer durchgeführt worden. Die Benutzung von force user und force group wird dies erreichen. In anderen Situationen ist es vielleicht notwendig, ein paranoides Maß an Kontrollen einzusetzen, um sicherzustellen, dass es nur bestimmten ausgewählten und autorisierten Personen möglich ist, auf eine Freigabe oder dessen Inhalt zuzugreifen. Hier kann die Benutzung von valid users oder invalid users am hilfreichsten sein.

Wie immer ist es höchst ratsam, die einfachste Methode für die Verwaltung und die eindeutigste Methode für die Zugriffskontrolle zu verwenden. Denken Sie daran, dass nach dem Verlassen Ihrer Arbeit jemand anderes Unterstützung geben können muss, und wenn er eine große Baustelle vorfindet oder Ihre Vorgehensweise nicht versteht, kann es durchaus möglich sein, dass Samba gelöscht wird oder eine alternative Lösung eingesetzt wird.

Tabelle **??** zählt diese Kontrollen auf.

12.3.2 Kontrollen, die auf Datei- und Verzeichnis-Berechtigungen basieren

Die folgenden auf Datei- und Verzeichnis-Berechtigungen basierenden Kontrollen können, wenn sie falsch angewendet werden, durch Fehlkonfigurationen zu erheblichen Schwierigkeiten bei der Fehlersuche führen. Benutzen Sie diese sparsam und sorgfältig. Durch die

Tabelle 12.2. Benutzer- und gruppen-basierende Kontrollen

Kontrollparameter	Beschreibung - Ausführung - Hinweise
admin users	Liste der Benutzer, denen Administrationsprivilegien auf der Freigabe erteilt werden. Sie werden alle Dateioperationen als Super-User (root) ausführen. Jeder Benutzer in dieser Liste wird in der Lage sein, alles auf der Freigabe zu machen, egal welche Dateiberechtigungen gesetzt wurden.
force group	Spezifiziert einen UNIX-Gruppennamen, der als primäre Standardgruppe allen Benutzern zugewiesen wird, die sich mit diesem Dienst verbinden.
force user	Spezifiziert einen UNIX-Benutzernamen, der als Standardbenutzer allen Benutzern zugewiesen wird, die sich mit diesem Dienst verbinden. Dies ist für das gemeinsame Nutzen von Dateien hilfreich. Die falsche Benutzung kann Sicherheitsprobleme verursachen.
guest ok	Falls dieser Parameter für einen Dienst gesetzt ist, wird kein Passwort verlangt, um sich mit diesem Dienst zu verbinden. Die Privilegien sind diejenigen des Gastzugangs.
invalid users	Liste der Benutzer, denen ein Anmelden an diesem Dienst nicht erlaubt wird.
only user	Kontrolliert, ob Verbindungen mit Benutzernamen, die nicht in der Liste enthalten sind, erlaubt werden.
read list	Liste der Benutzer, die einen Nur-Lesezugriff auf diesen Dienst haben. Benutzer in dieser Liste bekommen keinen Schreibzugriff, egal wie die Option 'read only' gesetzt wurde.
username	Sehen Sie in der `smb.conf`-Manpage für mehr Informationen nach – dies ist ein komplexer Parameter, der häufig falsch angewendet wird.
valid users	Lister der Benutzer, denen das Anmelden an diesem Dienst erlaubt wird.
write list	Liste der Benutzer, denen Lese-Schreibzugriff auf diesen Dienst erlaubt wird.

schrittweise Einführung einer Berechtigung nach der anderen können unerwünschte Nebeneffekte entdeckt werden. Im Fehlerfall kommentieren Sie alle aus und führen sie dann Schritt für Schritt in einer kontrollierten Art und Weise wieder ein.

In Tabelle **??** finden Sie Informationen, die diese Parameter betreffen.

12.3.3 Allgemeine Kontrollen

Das Folgende ist dokumentiert, da es weit verbreitet ist, dass Administratoren unabsichtlich Barrieren beim Einrichten von Dateizugriffen dadurch aufbauen, dass sie die genauen Auswirkungen von Dateieinstellungen in `smb.conf` nicht verstehen (siehe Tabelle **??**).

Tabelle 12.3. Auf Datei- und Verzeichnis-Berechtigungen basierende Kontrollen

Kontrollparameter	Beschreibung - Ausführung - Hinweise
create mask	Sehen Sie in der `smb.conf`-Manpage nach.
directory mask	Die Oktal-Modi, die beim Konvertieren von DOS-Modi in UNIX-Modi während des Erzeugens von UNIX-Verzeichnissen benutzt werden. Siehe auch: directory security mask.
dos filemode	Durch Einschalten dieses Parameters erlaubt man einem Benutzer, der Schreibzugriff auf eine Datei hat, die Berechtigungen auf diese zu ändern.
force create mode	Dieser Parameter spezifiziert eine Anzahl von UNIX-Mode-Bit-Berechtigungen, die immer auf eine Datei gesetzt werden, die durch Samba erzeugt wurde.
force directory mode	Dieser Parameter spezifiziert eine Anzahl von UNIX-Mode-Bit-Berechtigungen, die immer auf ein Verzeichnis gesetzt werden, das durch Samba erzeugt wurde.
force directory security mode	Kontrolliert Änderungen an UNIX-Berechtigungsbits, wenn ein Windows NT-Client UNIX-Berechtigungen eines Verzeichnisses manipuliert.
force security mode	Kontrolliert Änderungen an UNIX-Berechtigungsbits, wenn ein Windows NT-Client UNIX-Berechtigungen manipuliert.
hide unreadable	Verhindert, dass Clients die Existenz von Dateien sehen, die nicht lesbar sind.
hide unwriteable files	Verhindert, dass Clients die Existenz von Dateien sehen, die nicht schreibbar sind. Nicht beschreibbare Verzeichnisse werden wie gewöhnlich angezeigt.
nt acl support	Dieser Parameter kontrolliert, ob smbd versuchen wird, UNIX-Berechtigungen auf Windows NT-Zugriffsberechtigungslisten zu mappen.
security mask	Kontrolliert Änderungen an UNIX-Berechtigungsbits, wenn ein Windows NT-Client UNIX-Berechtigungen einer Datei manipuliert.

12.4 Zugriffskontrollen auf Freigaben

Dieses Kapitel handelt davon, wie Samba für Zugriffskontroll-Einschränkungen bei Freigaben konfiguriert werden kann. Standardmäßig setzt Samba keine Einschränkungen auf die Freigabe selbst. Einschränkungen auf der Freigabe selbst können auf MS Windows NT4/200x/XP-Freigaben gesetzt werden. Dies kann ein effektives Verfahren sein, um zu regeln, wer sich mit einer Freigabe verbinden darf. In Ermangelung spezifischer Einschränkungen sieht die Standardeinstellung vor, dem globalen Benutzer `Jeder - Volle Kontrolle` (volle Kontrolle, Ändern und Lesen) zu erlauben.

Zurzeit stellt Samba kein Werkzeug zum Konfigurieren von Zugriffskontroll-Einstellungen auf einer Freigabe selbst zur Verfügung. Samba hat die Fähigkeit, Zugriffskontroll-

Einstellungen zu speichern und damit zu arbeiten, aber der einzige Weg, diese Einstellungen zu erzeugen, ist der NT4 Server Manager oder die Windows 200x MMC für Computer-Verwaltung.

Samba speichert die Zugriffskontroll-Einstellungen pro Freigabe in einer Datei namens `share_info.tdb`. Der Ablageort dieser Datei auf Ihrem System hängt davon ab, wie Sie Samba kompiliert haben. Der Standard-Ablageort für Sambas tdb-Dateien ist `/usr/local/samba/var`. Falls das `tdbdump`-Werkzeug auf Ihrem System kompiliert und installiert worden ist, können Sie den Inhalt dieser Datei wie folgt ausführen: **tdbdump share_info.tdb**, in dem Verzeichnis, das die tdb-Dateien enthält.

12.4.1 Verwaltung von Freigabeberechtigungen

Das beste Werkzeug für eine Aufgabe ist plattformabhängig. Wählen Sie das beste Werkzeug für Ihre Umgebung.

12.4.1.1 Windows NT4 Workstation/Server

Das Werkzeug, das Sie zum Verwalten von Freigabeberechtigungen auf einem Samba-Server nutzen müssen, ist der NT Server Manager. Der Server Manager wird mit den Windows NT4 Server-Produkten, aber nicht mit Windows NT4 Workstation ausgeliefert. Sie können den NT Server Manager für MS Windows NT4 Workstation von Microsoft erhalten (Details weiter unten).

Anweisungen

1. Starten Sie den NT4 Server Manager, und klicken Sie auf den Samba-Server, den Sie administrieren möchten. In dem Menü wählen Sie **Computer**, dann klicken Sie auf **Freigegebene Verzeichnisse**.

2. Klicken Sie auf die Freigabe, die Sie verwalten möchten, dann gehen Sie auf **Eigenschaften** und klicken auf die Registerkarte **Berechtigungen**. Jetzt können Sie Zugriffskontroll-Einstellungen nach Belieben hinzufügen und ändern.

12.4.1.2 Windows 200x/XP

Auf MS Windows NT4/200x/XP werden Systemzugriffskontroll-Listen für Freigaben mit eigenen Werkzeugen gesetzt, meist durch den Dateimananger. In Windows 200x beispielsweise rechtsklicken Sie auf den Freigabeordner, wählen **Freigabe** und klicken dann auf **Berechtigungen**. Die Standardberechtigung unter Windows NT4/200x erlaubt „*jedem*“ volle Kontrolle über die Freigabe.

MS Windows 200x und spätere Versionen enthalten ein Werkzeug namens Computerverwaltungs-Snap-In für die Microsoft Management Konsole (MMC). Dieses Werkzeug befindet sich in der **Systemsteuerung** -> **Verwaltung** -> **Computerverwaltung**. Anweisungen

1. Nachdem Sie die MMC über das Computerverwaltungs-Snap-In gestartet haben, klicken Sie auf den Menüeintrag **Action** und wählen dann **Mit einem anderen Computer verbinden**. Falls Sie nicht an einer Domäne angemeldet sind, werden Sie aufgefordert, einen Domänenbenutzer und ein Passwort einzugeben. Dies wird Sie gegenüber der Domäne authentifizieren. Falls Sie bereits als ein Benutzer mit Administrationsrechten angemeldet sind, wird dieser Schritt nicht angeboten.

2. Falls der Samba-Server nicht in der Box **Computer auswählen** angezeigt wird, geben Sie den Namen des Samba-Zielservers im Feld **Name:** ein. Klicken Sie jetzt auf den Button **[+]** neben **Systemwerkzeuge**, dann auf den Button **[+]** neben **Freigabeordner** im linken Bereich.

3. Im rechten Bereich doppelklicken Sie auf die Freigabe, auf die Sie Zugriffskontroll-Berechtigungen vergeben möchten. Dann klicken Sie auf die Registerkarte **Freigabe-Berechtigungen**. Jetzt ist es möglich, Zugriffskontroll-Einheiten zu dem Freigabe-Ordner hinzuzufügen. Merken Sie sich, welchen Zugriffstyp (volle Kontrolle, ändern, lesen) Sie für jeden Eintrag vergeben möchten.

WARNUNG

Seien Sie vorsichtig. Falls Sie alle Berechtigungen von dem `Jeder` Benutzer wegnehmen, ohne diesen Benutzer entfernt zu haben, wird anschließend kein Benutzer mehr in der Lage sein, auf die Freigabe zuzugreifen. Dies ist ein Ergebnis dessen, was als ACL-Präzedenz bekannt ist. `Jeder` mit dem Eintrag *kein Zugriff* heißt, dass `MaryK`, die Teil der Gruppe `Jeder` ist, keinen Zugriff hat, obwohl ihr explizit volle Zugriffsrechte gegeben wurden.

12.5 MS Windows-Zugriffskontroll-Listen (ACLs) und UNIX-Wechselwirkungen

12.5.1 Verwalten von UNIX-Berechtigungen durch NT-Sicherheitsdialoge

Windows NT-Clients können ihre eigene Dialogbox für Sicherheitseinstellungen verwenden, um UNIX-Berechtigungen anzuzeigen und zu ändern.

Diese Fähigkeit ist so umsichtig, dass die Sicherheit des UNIX-Hosts, auf dem Samba läuft, nicht gefährdet wird und dennoch alle Dateiberechtigungsregeln, die ein Samba-Administrator setzt, beachtet werden.

Samba versucht nicht, die POSIX-ACLs zu übertreffen, so dass die vielen feiner abgestimmten Zugriffskontroll-Optionen, die Windows zur Verfügung stellt, einfach ignoriert werden.

ANMERKUNG

Alle Zugriffe auf UNIX/Linux-Systemdateien durch Samba werden durch die Betriebssystem-Dateizugriffskontrollen kontrolliert. Bei der Fehlersuche nach Dateizugriffsproblemen ist es enorm wichtig, die Identität des Windows-Benutzers herauszufinden, wie sie von Samba an dieser Stelle des Dateizugriffs gesehen wird. Diese kann am besten durch die Samba-Protokolldateien ermittelt werden.

12.5.2 Anzeigen von Dateisicherheit auf einer Samba-Freigabe

Von einem NT4/2000/XP-Client aus rechtsklicken Sie auf jede Datei oder Verzeichnis in einem Samba- gemounteten Laufwerksbuchstaben oder UNC-Pfad. Wenn das Menü aufgeht, klicken Sie auf den Eintrag **Eigenschaften** am Fuß des Menüs. Dies startet die Dialogbox `Eigenschaften`. Klicken Sie auf die Registerkarte **Sicherheit**, **Erweitert** und Sie werden drei Panels sehen: **Berechtigungen**, **Überwachung** und **Besitzer**. Der Button **Überwachung** wird entweder eine Fehlermeldung 'A requested privilege is not held by the client' verursachen,

falls der Benutzer kein NT-Administrator ist, oder einen Dialog erscheinen lassen, mit dem ein Administrator Überwachungsgrundlagen einer Datei hinzufügen kann, wenn der Benutzer als NT-Administrator angemeldet ist. Dieser Dialog funktioniert derzeit nicht mit einer Samba-Freigabe, da der einzige Button, der **Hinzufügen**-Button, es derzeit nicht zulässt, eine Benutzerliste anzuzeigen.

12.5.3 Anzeigen von Dateieigentümern

Wenn Sie auf den Button **Eigentümer** klicken, erscheint eine Dialogbox, die Ihnen zeigt, wem die betreffende Datei gehört. Der Name des Eigentümers wird wie folgt angezeigt:

„SERVER\Benutzer (Langer Name)“

SERVER ist der NetBIOS-Name des Samba-Servers, *Benutzer* der Name des UNIX-Benutzers, dem die Datei gehört, und *(Langer Name)* ist die Beschreibung, die den Benutzer ausweist (normalerweise wird dies im GECOS-Feld der UNIX-Passwortdatenbank gefunden). Klicken Sie auf den Button **Abbrechen**, um diesen Dialog zu entfernen.

Falls der Parameter nt acl support auf `false` gesetzt ist, wird der Dateieigentümer als NT-Benutzer *Jeder* angezeigt.

Mit dem **Übernehmen**-Button können Sie nicht die Eigentumsrechte an dieser Datei auf sich selbst setzen (ein Anklicken zeigt eine Dialogbox, die angibt, dass der Benutzer, als der Sie gerade auf dem NT-Client angemeldet sind, nicht gefunden werden kann). Der Grund hierfür ist, dass das Ändern der Eigentumsrechte auf eine Datei eine privilegierte Operation in UNIX ist, die ausschließlich dem Benutzer *root* obliegt. Indem Sie auf diesen Button klicken, veranlassen Sie NT dazu, die Eigentumsrechte einer Datei auf den am NT-Client gegenwärtig angemeldeten Benutzer zu übertragen; dies funktioniert jedoch zu diesem Zeitpunkt mit Samba nicht.

Es gibt ein NT-Kommando, **chown**, das mit Samba funktioniert und es einem Benutzer, der mit Administratorprivilegien an einen Samba-Server als root angeschlossen ist, erlaubt, die Eigentumsrechte von Dateien sowohl auf lokaler NTFS-Dateisystemebene als auch auf entfernt gemounteten NTFS- oder Samba-Laufwerken zu setzen. Dies ist verfügbar als Teil der von Jeremy Allison vom Samba-Team geschriebenen Seclib-NT-Sicherheitsbibliothek, und Sie können es von der FTP-Hauptseite von Samba abrufen.

12.5.4 Das Anzeigen von Datei- oder Verzeichnisberechtigungen

Der dritte Button ist die Schaltfläche **Berechtigungen**. Wenn Sie sie anklicken, öffnet sich eine Dialogbox, die sowohl die Berechtigungen als auch den UNIX-Besitzer für die Datei und das Verzeichnis anzeigen. Der Eigentümer wird wie folgt angezeigt:

SERVER\Benutzer (Langer Name)

SERVER ist der NetBIOS-Name des Samba-Servers, *Benutzer* ist der Name des UNIX-Benutzers, dem die Datei gehört, und *(Langer Name)* ist die Beschreibung, die den Benutzer ausweist (normalerweise wird dies im GECOS-Feld der UNIX-Passwortdatenbank gefunden).

Falls der Parameter nt acl support auf `false` gesetzt ist, wird der Dateieigentümer als NT-Benutzer *Jeder* angezeigt.

Das Berechtigungsfeld wird bei Dateien und Verzeichnissen anders dargestellt, also werde ich die Art, wie Dateiberechtigungen angezeigt werden, zuerst beschreiben.

12.5.4.1 Dateiberechtigungen

Die Standard-UNIX-Drillinge Benutzer/Gruppe/Welt und die korrespondierenden Berechtigungen `lesen, schreiben, ausführen` werden von Samba in ein aus drei Elementen bestehendes NT-ACL mit den Bits „*r*“, „*w*“ und „*x*“ von Samba in ein aus drei Elementen bestehendes NT-ACL gemappt, wobei die Bits „*r*“, „*w*“ und „*x*“ auf passende NT-Berechtigungen gemappt werden. Die UNIX-Welt-Berechtigungen werden in die globale NT-Gruppe `Jeder` gemappt, gefolgt von der Berechtigungsliste, die unter UNIX für Welt gilt. Die UNIX Eigentümer- und Gruppenberechtigungen werden als ein NT- **Benutzer**-Symbol und ein NT-Symbol **lokale Gruppe** angezeigt, beziehungsweise durch die nachfolgende Berechtigungsliste für den UNIX-Benutzer und die UNIX-Gruppe.

Dadurch, dass viele UNIX-Berechtigungssätze nicht auf allgemeine NT-Namen wie `lesen`, `ändern` oder `volle Kontrolle` passen, werden gemeinhin die Berechtigungen durch Wörter wie `Spezieller Zugriff` in der NT-Anzeigeliste angeführt.

Doch was passiert, wenn die Datei keine Berechtigungen für eine bestimmte UNIX-Benutzergruppe oder Welt-Komponente erlaubt? Um es zu ermöglichen, „*keine Berechtigungen*“ zu sehen und zu ändern, übergibt Samba das NT-ACL-Attribut `Eigentum übernehmen` (das keine Bedeutung für UNIX hat) und meldet eine Komponente ohne Berechtigung, wie wenn das NT-Bit **O** gesetzt wäre. Dies wurde natürlich deshalb gewählt, um es wie eine Null aussehen zu lassen, was bedeutet: Keine (Null) Berechtigungen. Weitere Details zu dieser Entscheidung werden weiter unten angeführt.

12.5.4.2 Verzeichnis-Berechtigungen

Verzeichnisse auf einem NTFS-Dateisystem haben zwei verschiedene Berechtigungssätze. Der erste Satz ist die ACL, die auf das Verzeichnis selbst gesetzt ist. Sie wird normalerweise im ersten Satz der Klammern im normalen NT-Stil `RW` angezeigt. Dieser erste Satz an Berechtigungen wird durch Samba in exakt derselben Art und Weise erzeugt, wie es normale Dateiberechtigungen werden, und wird auch auf diesselbe Art und Weise angezeigt.

Der zweite Satz von Verzeichnis-Berechtigungen hat keine echte Bedeutung in der UNIX-Berechtigungs-Welt und repräsentiert die `vererbten` Berechtigungen, die jede Datei erben würde, die in diesem Verzeichnis erzeugt wird.

Samba vereinigt diese vererbten Berechtigungen für NT, indem es die UNIX-Berechtigungsmodi als eine NT-ACL zurückgibt, so wie es eine Datei erhalten würde, die Samba für diese Freigabe erzeugt hat.

12.5.5 Ändern von Datei- oder Verzeichnis-Berechtigungen

Das Ändern von Datei- und Verzeichnis-Berechtigungen ist genauso einfach wie das Ändern der Anzeige der Berechtigungen in der Dialogbox und das Klicken auf **OK**. Jedoch gibt es Einschränkungen, die ein Benutzer kennen sollte und die mit den Standard-Samba-Berechtigungsmasken und mit dem Vergeben von DOS-Attributen zu tun haben, die ebenfalls in diesem Zusammenhang berücksichtigt werden müssen.

Falls der Parameter nt acl support auf `false` gesetzt ist, schlägt jeder Versuch, Sicherheitsberechtigungen zu setzen, mit einer Meldung 'Zugriff verweigert' fehl.

Das Erste, was anzumerken ist, ist, dass der Button **Hinzufügen** keine Samba-Benutzerliste zurückgeben wird (es wird eine Fehlermeldung ausgegeben, die besagt 'Der Remoteprozedur-Aufruf schlug fehl und konnte nicht ausgeführt werden'). Das bedeutet, dass Sie nur die gegenwärtigen Benutzer/Gruppen/Welt-Berechtigungen, die in der Dialogbox angezeigt werden, ändern können. Dies funktioniert deshalb so gut, weil es die einzigen Berechtigungen sind, die UNIX augenblicklich hat.

Falls ein Berechtigungsdrilling (entweder Benutzer, Gruppe oder Welt) von der Liste der Berechtigungen in der NT-Dialogbox entfernt wird und dann der **OK**-Button angeklickt wird, wird dies auf UNIX-Seite als „*keine Berechtigungen*“ angewendet. Wenn Sie sich dann die Berechtigungen nochmals ansehen, wird der Eintrag „*keine Berechtigungen*“ als das NT-Flag **O** wie oben beschrieben angezeigt. Dies erlaubt es Ihnen, Berechtigungen wieder auf eine Datei oder Verzeichnis zu setzen, nachdem Sie diese von einer der Drillingskomponenten entfernt hatten.

Weil UNIX nur die Bits „*r*“, „*w*“ und „*x*“ einer NT-ACL unterstützt, werden diese ignoriert, falls andere NT-Sicherheitsattribute wie `Löschzugriff` ausgewählt wurden, falls diese auf einem Samba-Server angewandt werden.

Wenn Berechtigungen auf ein Verzeichnis gesetzt werden, wird der zweite Satz an Berechtigungen (im zweiten Klammern-Paar) standardmäßig auf alle Dateien in diesem Verzeichnis angewandt. Falls Sie dies nicht wünschen, müssen Sie die Auswahlbox **Berechtigungen auf existierende Dateien zurücksetzen** in dem NT-Dialog vor einem Klicken auf **OK** abwählen.

Falls Sie es wünschen, alle Berechtigungen von einer Benutzer/Gruppe/Welt-Komponente zu entfernen, können Sie entweder eine Komponente auswählen und auf den Button **Entfernen** klicken, oder setzen Sie die Komponente darauf, nur die spezielle Berechtigung `Berechtigung übernehmen` (angezeigt als **O**) zu setzen.

12.5.6 Die Wechselwirkung mit den Samba-Standard-Parametern „*create mask*“

Es gibt vier Parameter, die das Wechselspiel mit den Samba-Standard-Parametern *`create mask`* kontrollieren. Diese sind:

- security mask
- force security mode
- directory security mask

- force directory security mode

Sobald ein Benutzer auf **OK** klickt, um Berechtigungen zu setzen, mappt Samba die angegebenen Berechtigungen in einen Benutzer/Gruppe/Welt-Drillingssatz und gleicht dann die geänderten Berechtigungen für diese Datei mit den in security mask gesetzten Bits ab. Jedes geänderte Bit, das nicht mit „*1*“ in diesem Parameter gesetzt wurde, bleibt in den Dateiberechtigungen unberücksichtigt.

Grundsätzlich werden Null-Bits in der security mask als ein Satz von Bits behandelt, die der Benutzer *nicht* ändern darf, Einer-Bits darf der Benutzer ändern.

Falls er nicht ausdrücklich gesetzt worden ist, zeigt dieser Parameter standardmäßig auf denselben Wert wie der Parameter create mask. Um es einem Benutzer zu erlauben, alle Berechtigungen von Benutzer/Gruppe/Welt an einer Datei zu ändern, setzen Sie diesen Parameter auf 0777.

Als Nächstes gleicht Samba die geänderten Berechtigungen einer Datei mit den Bits ab, die im force security mode-Parameter gesetzt sind. Jedes geänderte Bit wird passend zu den auf „*1*“ gesetzten Bits in diesem Parameter zwangsläufig gesetzt.

Grundsätzlich werden Bits aus dem Parameter *force security mode* als ein Satz von Bits behandelt, die der Benutzer immer auf „*an*“ gesetzt hat, wenn die Sicherheit einer Datei geändert wird.

Falls er nicht ausdrücklich gesetzt worden ist, zeigt dieser Parameter standardmäßig auf denselben Wert wie der Parameter force create mode. Um es einem Benutzer zu erlauben, alle Berechtigungen von Benutzer/Gruppe/Welt an einer Datei ohne Berechtigungen zu ändern, setzen Sie diesen Parameter auf 000. Die Parameter security mask und *force security mode* werden angewendet, um die Anfragen in dieser Reihenfolge zu ändern.

Für ein Verzeichnis wird Samba dieselben Operationen durchführen, wie zuvor für eine Datei beschrieben. Es wird jedoch der Parameter *directory security mask* anstatt des Parameters *security mask* und Parameter *force directory security mode* anstatt des Parameters *force security mode* angewandt.

Der Parameter directory security mask ist standardmäßig auf denselben Wert wie der Parameter *directory mask* gesetzt, und der Parameter *force directory security mode* ist standardmäßig auf denselben Wert wie der Parameter force directory mode gesetzt. Auf diese Weise erzwingt Samba die Einschränkungen bei Berechtigungen, die ein Administrator auf einer Samba-Freigabe gesetzt hat, während den Benutzern weiterhin erlaubt wird, innerhalb dieser Einschränkung die Berechtigungsbits zu ändern.

Falls Sie eine Freigabe aufsetzen möchten, die es Benutzern erlaubt, die volle Kontrolle bei der Änderung von Berechtigungsbits auf ihren eigenen Dateien und Verzeichnissen auszuüben, und die es nicht erfordert, irgendwelche Bits auf „*an*“ zu verstellen, dann setzen Sie die folgenden Parameter in der `smb.conf` Datei innerhalb des freigabe-spezifischen Abschnitts:

```
security mask = 0777
force security mode = 0
directory security mask = 0777
force directory security mode = 0
```

12.5.7 Die Wechselwirkung mit den Standard-Samba-Dateiattribut-Vergaben

ANMERKUNG

Samba vergibt einige der DOS-Attribut-Bits (wie z.B. „*Nur lesen*“) in den UNIX-Berechtigungen einer Datei. Dies bedeutet, dass es einen Konflikt zwischen den Berechtigungsbits, die durch den Sicherheitsdialog gesetzt wurden, und den Berechtigungen geben kann, die durch die Vergabe von Dateiattributen gesetzt wurden.

Falls eine Datei für den Eigentümer keinen UNIX-Lesezugriff hat, wird diese als „*Nur lesen*“ in dem Standarddialog der Registerkarte **Dateiattribute** angezeigt. Leider ist dieser Dialog derselbe, der die Sicherheitsinformationen in einer anderen Registerkarte enthält.

Der Eigentümer kann dadurch fälschlicherweise glauben, die Berechtigungen dadurch ändern zu können, weil es ihm anscheinend erlaubt wird, Lesezugriff durch Nutzung des Sicherheitsdialoges zu bekommen; er klickt auf **OK**, um zurück zu der Registerkarte mit den Standardattributen zu gelangen, klickt auf **OK** in diesem Dialog, und NT setzt die Dateiberechtigungen auf Nur-lesen zurück (weil dies die Attribute in diesem Dialog ihm sagen). Dies bedeutet: Klicken Sie - nachdem Sie die Berechtigungen gesetzt und auf **OK** zum Zurückgehen auf den Attributdialog geklickt haben - immer auf **Abbrechen** statt auf **OK**, um sicherzustellen, dass Ihre Änderungen nicht überschrieben werden.

12.6 Gängige Fehler

Datei-, Verzeichnis- und Freigabezugriffsprobleme tauchen häufig auf der Mailingliste auf. Die folgenden Beispiele wurden in letzter Zeit in der Maillingliste behandelt.

12.6.1 Benutzer können nicht auf eine öffentliche Freigabe schreiben

„*Wir haben einige Schwierigkeiten mit Datei/Verzeichnis-Berechtigungen. Ich kann mich als Admin-User (root) an einer Domäne anmelden, und es gibt eine öffentliche Freigabe, auf der jeder die Berechtigung zum Erzeugen und Ändern von Dateien haben sollte, aber nur root kann Dateien ändern, sonst niemand. Wir müssen dauernd auf dem Server* `chgrp -R users *` *und* `chown -R nobody *` *eingeben, um den anderen Benutzern das Ändern von Dateien zu erlauben.*“

Es gibt viele Möglichkeiten, dieses Problem zu lösen, und hier sind ein paar Hinweise:

1. Gehen Sie auf die oberste Ebene des Verzeichnisses, das freigegeben ist.
2. Setzen Sie die Benutzer und Gruppe als Eigentümer auf das, was öffentlich sein soll

```
$ find 'directory_name' -type d -exec chown user.group {}\;
```

```
$ find 'directory_name' -type d -exec chmod 6775 'directory_name'
$ find 'directory_name' -type f -exec chmod 0775 {} \;
$ find 'directory_name' -type f -exec chown user.group {}\;
```

> ANMERKUNG
>
>
>
> Das oben Aufgeführte setzt das `Sticky-Bit` auf alle Verzeichnisse. Lesen Sie in Ihren UNIX/Linux-Manpages nach, was dies bewirkt. Es veranlasst das Betriebssystem, auf alle Dateien in Ihren Verzeichnissen den Eigentümer des Verzeichnisses zu setzen.

3. Das Verzeichnis heißt: */foobar*

```
$ chown jack.engr /foobar
```

> ANMERKUNG
>
>
>
> Dies ist dasselbe wie:
>
> ```
> $ chown jack /foobar
> $ chgrp engr /foobar
> ```

4. Geben Sie jetzt Folgendes ein:

```
$ chmod 6775 /foobar
$ ls -al /foobar/..
```

Dann sollten Sie dies sehen:

```
drwsrwsr-x  2 jack  engr    48 2003-02-04 09:55 foobar
```

5. Geben Sie jetzt dies ein:

```
$ su - jill
$ cd /foobar
```

```
$ touch Afile
$ ls -al
```

Sie sollten nun sehen, dass die Datei `Afile`, die von Jill erzeugt worden ist, die Eigentumsrechte und Berechtigungen von Jack hat, so wie hier:

```
-rw-r--r--  1 jack  engr     0 2003-02-04 09:57 Afile
```

6. Fügen Sie jetzt in Ihrer `smb.conf` für die Freigabe Folgendes ein:

```
force create mode = 0
force directory mode
```

> ANMERKUNG
>
>
>
> Diese Maßnahmen werden nur dann gebraucht, wenn Ihre Benutzer nicht Mitglied der Gruppe sind, die Sie benutzt haben. Das ist dann der Fall, wenn Sie innerhalb des Betriebssystems keine Schreibberechtigung auf das Verzeichnis haben.

Eine Alternative ist es, in der `smb.conf` diesen Eintrag für die Freigabe zu setzen:

```
force user = jack
force group = engr
```

12.6.2 Dateioperationen, die als *root* mit *force user* ausgeführt wurden

Wenn Sie einen Benutzer in admin users haben, wird Samba für diesen Benutzer Dateioperationen immer als *root* ausführen, sogar wenn force user gesetzt wurde.

12.6.3 MS Word mit Samba ändert den Eigentümer einer Datei

Frage: „Wenn Benutzer B ein Word-Dokument abspeichert, das Benutzer A gehört, ist anschließend der Eigentümer der aktualisierten Datei Benutzer B. Warum macht Samba das? Wie kann ich das beheben?“

Antwort: Word macht Folgendes, wenn Sie ein Word-Dokument ändern: Es erzeugt ein NEUES Dokument mit einem temporären Namen. Word schließt dann das alte Dokument und löscht es. Dann benennt Word das neue Dokument in den Original-Dateinamen um. Es gibt keinen Mechanismus, durch den Samba in irgendeiner Weise wissen kann, dass das neue Dokument wirklich dem Eigentümer der Originaldatei gehören sollte. Samba hat keine Möglichkeit zu erfahren, dass MS Word die Datei umbenannt hat. Samba ist nur in der Lage zu sagen, dass die Datei, die erzeugt wurde, eine NEUE Datei ist, aber nicht, dass die Applikation (Word) diese aktualisiert hat.

Es gibt einen Workaround, um diese Berechtigungsprobleme zu lösen. Dieser Workaround setzt voraus, dass Sie verstehen, wie Sie das Verhalten des Dateisystems innerhalb der Datei

`smb.conf` steuern können, und wissen, wie ein UNIX-Dateisystem funktioniert. Setzen Sie **chmod g+s 'directory_name'** auf das Verzeichnis, in dem Sie Word-Dokumente ändern möchten. Dies stellt sicher, dass alle Dateien mit der Gruppe erzeugt werden, der das Verzeichnis gehört. In dem Abschnitt in der `smb.conf`, der die Freigabe deklariert, setzen Sie:

```
force create mode = 0660
force directory mode = 0770
```

Diese beiden Einstellungen stellen sicher, dass alle Verzeichnisse und Dateien, die in der Freigabe erzeugt werden, durch den Eigentümer und die Gruppe les- und schreibbar sind, die auf das Verzeichnis selbst gesetzt sind.

Tabelle 12.4. Andere Kontrollen

Kontrollparameter	Beschreibung - Ausführung - Hinweise
case sensitive, default case, short preserve case	Dies bedeutet, dass alle Dateinamensanzeigen in case-sensitiver Art erfolgen. Die Dateien werden genau so mit dem exakten Namen angelegt, wie Samba den Dateinamen vom Windows-Client erhält.
csc policy	Client-seitige Caching-Richtlinie - ermöglicht parallele MS Windows client-seitige Datei-Caching-Fähigkeiten.
dont descend	Erlaubt das Spezifizieren einer kommatagetrennten Verzeichnisliste, die der Server immer leer anzeigt.
dos filetime resolution	Diese Option ist hauptsächlich als Kompatibilitätsoption für Visual C++ gedacht, wenn dieses auf einer Samba-Freigabe genutzt wird.
dos filetimes	DOS und Windows erlauben Benutzern, Zeitstempel auf Dateien zu ändern, wenn diese auf die Datei schreiben können. POSIX-Semantiken verhindern dies. Diese Option erlaubt DOS- und Windows-Verhalten.
fake oplocks	Oplocks sind das Verfahren, wie SMB-Clients die Erlaubnis eines Servers bekommen, Dateioperationen lokal zu cachen (zwischenzuspeichern). Falls ein Server Oplocks erlaubt, ist es dem Client freigestellt anzunehmen, dass er der einzige ist, der auf die Datei zugreift, und er kann das Datei-Caching aggressiv nutzen.
hide dot files, hide files, veto files	Hinweis: MS Windows Explorer erlaubt das Überschreiben von Dateien, die als versteckt markiert sind, so dass sie weiter sichtbar sind.
read only	Falls dieser Parameter 'yes' ist, können Benutzer eines Dienstes Dateien im Dienste-verzeichnis weder erzeugen noch ändern.
veto files	Liste von Dateien oder Verzeichnissen, die nicht sichtbar sind und auf die man auch nicht zugreifen kann.

Kapitel 13

DATEI- UND SATZSPERREN

Ein Bereich, der vielen Netzwerkadministratoren Probleme verursacht, sind Sperren. Das Ausmaß des Problems ist bereits durch Recherchen über das Internet bewiesen.

13.1 Eigenschaften und Vorzüge

Samba bietet alle Sperrsemantiken, die MS Windows-Clients erwarten und die MS Windows NT/200x-Server auch zur Verfügung stellen.

Der Ausdruck *Sperren* (entsprechend dem etwas treffenderen englischen Begriff *Locking*, Anm. d. Übers.) hat grundsätzlich eine weite Bedeutung und deckt eine Vielzahl von Funktionen ab, die alle unter diesem einen Begriff zusammengefasst sind.

Opportunistisches Sperren ist ein wünschenswertes Feature, wenn es die wahrnehmbare Geschwindigkeit von Anwendungen auf einem Netzwerkclient beschleunigen kann. Jedoch ist das opportunistische Sperrprotokoll nicht robust, und deshalb können Probleme entstehen, wenn es von einer einfachen Konfiguration oder in einem sehr langsamen oder fehlerhaften Netzwerk aufgerufen wird. In diesen Fällen können der Aufwand für die Verwaltung der opportunistischen Sperren, die vom Betriebssystem durchgeführt wird, und der Aufwand für das Wiederherstellen nach Fehlern den erzielten Performance-Zuwachs wieder zunichte machen.

Der MS Windows-Netzwerkadministrator muss sich darüber im Klaren sein, dass Datei- und Satzsperren-Semantiken (Verhalten) entweder in Samba kontrolliert werden können oder durch Registry-Einstellungen auf einem MS Windows-Client.

ANMERKUNG

Manchmal ist es sogar notwendig, Einstellungen zu Sperrkontrollen sowohl auf dem Samba-Server als auch auf dem MS Windows-Client abzuschalten!

13.2 Erörterung

Es gibt zwei Arten von Sperren, die durch einen SMB-Server durchgeführt werden müssen. Die erste ist die *Satzsperre*, die einem Client das Sperren eines Bereichs von Bytes innerhalb einer geöffneten Datei erlaubt. Die zweite sind die *Verbotszustände (deny modes)*, die spezifiziert werden, wenn eine Datei geöffnet ist.

Satzsperren-Semantiken unter UNIX sind etwas vollkommen anderes als Satzsperren unter Windows. Samba-Versionen vor 2.2 hatten versucht, den nativen UNIX-Systemaufruf fcntl() zu nutzen, um saubere Satzsperren zwischen den verschiedenen Samba-Clients zu implementieren. Dies kann allerdings aus mehreren Gründen nicht vollständig richtig sein. Der einfachste Grund ist die Tatsache, dass ein Windows-Client einen Byte-Bereich von bis zu 2^32 oder 2^64 (je nach Client-Betriebssystem) sperren darf. Die UNIX-Sperren unterstützen nur einen Byte-Bereich bis zu 2^31. So ist es nicht möglich, eine Sperranfrage oberhalb von 2^31 sauber zu ermöglichen. Es gibt noch wesentlich mehr Unterschiede, zu viele, um hier alle aufzuführen.

Samba 2.2 und jüngere Versionen implementieren Satzsperren völlig unabhängig vom darunterliegenden UNIX-System. Wenn eine Byte-Bereichssperre, die ein Client anfordert, in den Bereich von 0-2^31 fällt, gibt Samba diese Anfrage an das UNIX-System weiter. Alle anderen Sperren können von UNIX jedoch nicht gesehen werden.

Vereinfacht ausgedrückt, sollte ein SMB-Server vor jedem Lese- und Schreibzugriff auf eine Datei nach Sperren suchen. Leider kann dies durch die Art und Weise, wie fcntl() arbeitet, langsam sein und den **rpc.lockd** überbeanspruchen. Dies ist fast immer unnötig, da von den Clients erwartet wird, dass sie unabhängig Sperr-Aufrufe vor Lese- und Schreibzugriffen absetzen, wenn das Sperren für sie wichtig ist. In der Voreinstellung setzt Samba nur dann Sperr-Aufrufe, wenn es explizit von einem Client danach gefragt wird; aber wenn Sie die Option strict locking = yes setzen, wird es diese Aufrufe bei *jedem* Lese- und Schreibzugriff ausführen.

Sie können das Sperren von Byte-Bereichen auch komplett abschalten, indem Sie locking = no setzen. Das ist hilfreich für jene Freigaben, die die Sperren nicht unterstützen oder sie nicht brauchen (wie CD-ROMs). In diesem Fall bildet Samba die Antwort-Codes von Sperr-Aufrufen nach, um den Clients mitzuteilen, dass alles in Ordnung ist.

Die zweite Klasse der Sperren sind die so genannten *deny modes*. Diese werden von einer Applikation gesetzt, wenn diese eine Datei öffnet, um zu bestimmen, welche Zugriffsarten gleichzeitig mit dieser Öffnung zu erlauben sind. Ein Client könnte nach `DENY_NONE`, `DENY_READ`, `DENY_WRITE` oder `DENY_ALL` fragen. Es gibt auch spezielle Kompatibilitätsmodi namens `DENY_FCB` und `DENY_DOS`.

13.2.1 Überblick über opportunistische Sperren

Das opportunistische Sperren, auch bezeichnet als „*Oplocks*“ (entspricht „*Opportunistic locking*“) wird vom Windows-Dateisystem über Registrierungseinträge aufgerufen (im Gegensatz zu einer API), um die Netzwerk-Performance zu erhöhen, wenn auf eine Datei auf einem Server zugegriffen wird. Die Performance wird durch lokales Puffern der Datei auf dem Client erhöht, was Folgendes erlaubt:

Read-ahead: Der Client liest die lokale Kopie der Datei, dadurch wird die Netzwerk-Latenz eliminiert.

Write caching: Der Client schreibt in die lokale Kopie der Datei, dadurch wird die Netzwerk-Latenz eliminiert.

Lock caching: Der Client puffert die Sperren der Anwendung lokal, und wieder wird die Netzwerk-Latenz eliminiert.

Die Performance-Steigerung von Oplocks kommt von der Möglichkeit des exklusiven Zugriffs auf die Datei — sogar wenn sie über `DENY_NONE` geöffnet ist — , da Windows den Status der Datei auf konkurrierende Zugriffe von anderen Prozessen überwacht.

Windows definiert vier Arten von Oplocks:

Level1 Oplock Der Redirektor sieht, dass die Datei mit DENY_NONE geöffnet wurde (was konkurrierende Zugriffe erlaubt), prüft, ob auch kein anderer Prozess auf die Datei zugreift, und prüft, dass Oplocks aktiviert sind. Dann gewährt er DENY_ALL/R+W/Exklusiv-Zugriff auf die Datei. Der Client führt seine Operationen nun auf die gepufferte Datei durch.

Wenn ein zweiter Prozess nun versucht, die Datei zu öffnen, wird das Öffnen verzögert, während der Redirektor den originalen Oplock „*aufbricht*“. Dieser Bruch des Oplocks signalisiert dem puffernden Client, die gepufferte Datei zurück auf den Server zu schreiben, die lokalen Sperren zu löschen und die Read-ahead-Daten zu verwerfen. Der Bruch ist dann komplett, die verzögerte Öffnung wird gewährt, und mehrere Prozesse können konkurrierenden Dateizugriff genießen, wie er von den Byte-Bereichs- oder den zwingenden Sperren diktiert wird. Wenn jedoch der originale öffnende Prozess die Datei in einem anderen Modus als DENY_NONE geöffnet hat, wird dem zweiten Prozess nur eingeschränkter oder gar kein Zugriff gewährt, trotz des Bruchs des Oplocks.

Level2 Oplock Arbeitet wie ein Level1 Oplock, außer dass nur Lesezugriffe gepuffert werden. Alle anderen Operationen werden auf der Server-Kopie der Datei durchgeführt.

Filter Oplock Erlaubt keinen Schreib- oder Löschzugriff auf Dateien.

Batch Oplock Manipuliert das Öffnen und Schließen von Dateien und erlaubt das Puffern von Dateiattributen.

Ein wichtiges Detail ist, dass Oplocks vom Dateisystem aufgerufen werden, nicht von einer Anwendungs-API. Daher kann eine Applikation eine opportunistisch gesperrte Datei schließen, aber das Dateisystem gibt den Oplock nicht auf. Wenn der Bruch des Oplocks durchgeführt wird, schließt das Dateisystem einfach die Datei in Vorbereitung auf das folgende Öffnen der Datei durch den zweiten Prozess.

Opportunistisches Sperren ist eigentlich ein unpassender Name für dieses Feature. Der wirkliche Nutzen dieses Features ist das Puffern von Daten („*Cachen*“) auf Client-Seite, und die Oplocks sind nur ein Mitteilungsmechanismus für das Zurückschreiben von Daten auf die Platte des Netzwerk-Servers. Die Einschränkung der Oplocks ist die Zuverlässigkeit des Mechanismus, einen Oplock-Bruch (Mitteilung) zwischen dem Server und dem puffernden Client auszuführen. Wenn dieser Austausch fehlerhaft abläuft (üblicherweise wegen eines Timeouts aus irgendwelchen Gründen), dann geht der Nutzen des client-seitigen Pufferns verloren.

Die tatsächliche Entscheidung, die ein Anwender oder Administrator erwägen sollte, ist, ob es vernünftig ist, unter mehreren Anwendern Daten zu teilen, die lokal auf den Clients gepuffert werden. In vielen Fällen ist die Antwort „*Nein*“. Zu entscheiden, wann Daten gepuffert werden und wann nicht, das ist hier die Frage, und daher sollte „*opportunistisches Sperren*“ als Schalter für client-seitiges Puffern behandelt werden. Schalten Sie es „*on*“, wenn client-seitiges Puffern erwünscht und zuverlässig ist. Schalten Sie es „*off*“, wenn client-seitiges Puffern redundant, unzuverlässig oder kontraproduktiv ist.

Opportunistisches Sperren wird von Samba standardmäßig für alle Freigaben auf „*on*“ gesetzt, also sollten Sie in jedem Fall vorsichtig vorgehen, um zu bestimmen, ob der potenzielle Nutzen die potenziellen Verzögerungen wert ist. Die folgenden Empfehlungen sollen Ihnen dabei helfen, eine Umgebung zu charakterisieren, in der opportunistische Sperren effektiv eingerichtet werden können.

Die Windows-Oplocks sind ein leichtgewichtiges performance-steigerndes Feature. Sie sind kein robustes und zuverlässiges Protokoll. Jede Implementierung von Oplocks sollte als Kompromiss zwischen Performance und Zuverlässigkeit geprüft werden. Die Zuverlässigkeit sinkt mit jeder oben genannten Regel, die nicht erzwungen wird. Stellen Sie sich einen Hochverfügbarkeits-Server auf einem Atoll im Südpazifik vor, der über ein WAN eine „*mission-critical*“ Multi-User-Firmen-Datenbank bereitstellt, und das auf einer Freigabe mit aktivierten Oplocks, während eines tropischen Sturms. Diese Konfiguration wird sehr wahrscheinlich Probleme mit Oplocks erfahren.

Oplocks können sehr wirksam die Client-Performance steigern, wenn sie als Konfigurationsschalter für client-seitiges Daten-Puffern behandelt werden. Wenn das Puffern der Daten wahrscheinlich unterbrochen werden könnte, sollte der Einsatz von Oplocks nochmals überdacht werden. Samba aktiviert standardmäßig die Verwendung von Oplocks auf allen Freigaben. Die client-seitige Verwendung von Daten auf dem Server, die Zuverlässigkeit des Servers im Netzwerk und die Oplock-Konfiguration jeder Freigabe sollten mit besonderer Aufmerksamkeit bedacht und konfiguriert werden. In Hochverfügbarkeitsumgebungen hat die Integrität der Daten oft hohe Priorität. Komplexe und teure Konfigurationen werden implementiert, um zu gewährleisten, dass sofort ein Ersatz verfügbar ist, wenn ein Client die Verbindung zum Dateiserver verliert, damit die durchgehende Verfügbarkeit der Daten gewährleistet ist.

Das Verhalten von Windows-Clients bei Ausfällen birgt ein höheres Risiko von Anwendungsunterbrechungen als das Verhalten anderer Plattformen, da es von einer aufgebauten TCP-Transport-Verbindung abhängt. Wenn die Verbindung unterbrochen wird — wie bei einem Datei-Server-Ausfall und dessen Ersatz durch einen Failover-Server — , muss eine neue Verbindung aufgebaut werden. Es ist selten, dass eine Windows-Client-Applikation so programmiert ist, dass sie sich korrekt von einer unterbrochenen Transport-Verbindung

erholt. Daher werden die meisten Applikationen in irgendeiner Art unterbrochen — im schlimmsten Fall abgebrochen, und erfordern einen Neustart.

Wenn eine Client-Session Schreib- und Lese-Vorgänge mit Oplocks lokal gepuffert hat, ist es wahrscheinlich, dass die Daten verloren gehen, wenn die Applikation neu startet oder sich nach der TCP-Unterbrechung wieder verbindet. Wenn die TCP-Verbindung ausfällt, ist der Status des Clients verloren. Wenn der Server die Verbindung wiederherstellt, wird keine Aufforderung zum Brechen des Oplocks an den Client gesandt. In diesem Fall ist die Arbeit aus der vorangegangenen Session verloren. Durch Echtzeit-Überwachung dieses Szenarios mit deaktivierten Oplocks und des Clients, der Daten auf den Datei-Server schreibt, wird die Ausfallsicherung die Daten auf der Platte so bewahren, wie sie zum Zeitpunkt des Verbindungsabbruchs existiert haben.

In „*mission-critical*“ Hochverfügbarkeitsumgebungen sollte große Vorsicht im Umgang mit Oplocks geübt werden. Idealerweise sollten umfassende Tests mit allen betroffenen Applikationen erfolgen, sowohl mit als auch ohne aktivierte Oplocks.

13.2.1.1 Exklusive Freigaben

Opportunistische Sperren sind am effektivsten, wenn sie auf Freigaben beschränkt sind, auf die ausschließlich ein einzelner Anwender zugreift oder nur ein Anwender gleichzeitig. Da der eigentliche Wert der Oplocks das client-seitige Puffern von Daten ist, verursacht jede Operation, die den Puffer-Mechanismus unterbricht, eine Verzögerung.

Home-Verzeichnisse sind die offensichtlichsten Beispiele für das sichere Realisieren von Performanc-Steigerungen mit Oplocks.

13.2.1.2 Freigaben oder Dateien, auf die von mehreren Usern zugegriffen wird

Mit jedem weiteren Anwender, der auf eine Datei auf einer Freigabe mit aktiven Oplocks zugreift, erhöht sich das Potenzial für Verzögerungen und eine daraus resultierende Performance-Verschlechterung. Wenn mehrere Anwender auf eine Datei auf einer Freigabe mit aktiven Oplocks zugreifen, übersteigt der Verwaltungsaufwand für das Senden und Empfangen der Oplock-Breaks und die resultierende Latenz, während die anderen Clients auf den momentan puffernden Client warten (bis er seine Puffer geleert hat), den Performance-Gewinn des puffernden Clients.

Mit jedem weiteren Client, der auf eine Datei mit gesetzten Oplocks zugreift, wird der potenzielle Performance-Zuwachs negiert, und es ergibt sich eventuell sogar ein Flaschenhals.

13.2.1.3 Dateien, auf die von UNIX- oder NFS-Clients aus zugegriffen wird

Lokale UNIX- oder NFS-Clients greifen ohne einen zwingenden Datei-Sperren-Mechanismus auf Dateien zu. Daher sind diese Client-Plattformen nicht imstande, vom Server aus einen Oplock-Bruch am Client zu erfragen, der gerade eine Datei puffert. Ein lokaler UNIX- oder NFS-Dateizugriff kann daher in eine Datei schreiben, die von einem Windows-Client gepuffert wurde, was diese Datei sehr wahrscheinlich unbrauchbar macht.

Wenn Dateien sowohl an Windows-Clients als auch an lokale UNIX- oder NFS-Benutzer freigegeben werden, sollten Sie das opportunistische Sperren abschalten.

13.2.1.4 Langsame und/oder unzuverlässige Netzwerke

Der größtmögliche Performance-Gewinn für Oplocks wird dann erzielt, wenn das client-seitige Puffern der Lese- und Schreib-Vorgänge den größten Unterschied zum Senden dieser Vorgänge über das Netzwerk liefert. Dies passiert am wahrscheinlichsten dann, wenn das Netzwerk extrem langsam, verstopft oder weit verteilt (wie in einem WAN) ist. Die Netzwerk-Latenz hat jedoch auch einen großen Einfluss auf die Zuverlässigkeit des Oplock-Bruch-Mechanismus und erhöht daher die Wahrscheinlichkeit, Oplock-Probleme zu bekommen, die die potenziellen Performance-Gewinne mehr als zunichte machen. Wenn natürlich niemals ein Oplock-Bruch gesendet werden müsste, wäre dies das vorteilhafteste Szenario, um Oplocks einzusetzen.

Wenn das Netzwerk langsam, unzuverlässig oder ein WAN ist, sollten Sie keine Oplocks konfigurieren, falls irgendeine Möglichkeit besteht, dass mehrere Benutzer regelmäßig dieselbe Datei öffnen.

13.2.1.5 Mehrbenutzer-Datenbanken

Mehrbenutzer-Datenbanken stellen klarerweise durch ihre grundlegende Natur ein Risiko dar — auf sie wird üblicherweise massiv von vielen Anwendern in zufälligen Intervallen zugegriffen. Das Platzieren einer Mehrbenutzer-Datenbank auf einer Freigabe mit aktivierten Oplocks wird wahrscheinlich zu einem Flaschenhals auf dem Samba-Server führen, weil die Sperren verwaltet werden müssen. Egal, ob eine Datenbank eine Eigenentwicklung ist oder ein kommerzielles Produkt, stellen Sie sicher, dass die entsprechende Freigabe deaktivierte Oplocks hat.

13.2.1.6 PDM-Daten-Freigaben

Process Data Management-(PDM-)Applikationen wie IMAN, Enovia und Clearcase finden immer mehr Verwendung mit Windows-Client-Plattformen und daher auch mit SMB-Daten-Servern. PDM-Applikationen verwalten Mehrbenutzer-Umgebungen für die Sicherheit von und den Zugriff auf kritische Daten. Die typische PDM-Umgebung ist üblicherweise mit ausgeklügelt entworfenen Client-Anwendungen verbunden, die Daten bei Bedarf lokal laden. Zusätzlich überwacht die PDM-Applikation üblicherweise den Daten-Status jeden Clients. In diesem Fall wird das client-seitige Puffern am besten der lokalen Applikation und dem PDM-Server überlassen. Es ist angemessen, das Client-OS von jeglichen Puffer-Aufgaben zu befreien, und auch den Server von der Verwaltung der Oplocks, indem man Oplocks auf der Freigabe deaktiviert.

13.2.1.7 Vorsicht vor Force User

Samba enthält einen Parameter in `smb.conf` namens force user, der den Benutzer, der auf eine Freigabe zugreift, vom tatsächlich zugreifenden Benutzer auf den in diesem Parameter angegebenen ändert. Wenn Oplocks auf einer Freigabe aktiviert sind, verursacht

die Änderung des Benutzers, dass ein Bruch des Oplocks an den Client gesendet wird, sogar wenn der Benutzer gar nicht explizit eine Datei geladen hat. In den Fällen, wo das Netzwerk langsam oder unzuverlässig ist, kann ein Oplock-Bruch verloren gehen, ohne dass der Benutzer auch nur auf eine Datei zugreift. Das kann sichtbare Performance-Einbrüche verursachen, wenn der Client wiederholt neu verbindet, um den verlorenen Oplock-Bruch „*zu überwinden*".

Vermeiden Sie die folgende Kombination:

- force user in der `smb.conf`-Freigaben-Konfiguration
- Langsames oder unzuverlässiges Netzwerk
- Opportunistisches Sperren aktiviert

13.2.1.8 Erweiterte Samba-Oplock-Parameter

Samba bietet Oplock-Parameter, die es dem Administrator erlauben, verschiedene Eigenschaften des Oplock-Mechanismus an Timing- und Benutzungs-Level anzupassen. Diese Parameter bieten hohe Flexibilität, um Oplocks in Umgebungen zu implementieren, wo sie sehr wahrscheinlich Probleme verursachen würden. Die Parameter sind: oplock break wait time und oplock contention limit.

Falls diese Parameter benötigt werden, ist es für die meisten Anwender, Administratoren und Umgebungen die bessere Wahl, die Oplocks einfach abzuschalten. Der Samba-SWAT-Hilfetext für diese beiden Parameter sagt: „*Do not change this parameter unless you have read and understood the Samba oplock code.*" Dies ist ein guter Rat.

13.2.1.9 Missionskritische Hochverfügbarkeit

In Hochverfügbarkeitsumgebungen ist die Integrität der Daten oft von hoher Priorität. Komplexe und teure Konfigurationen werden implementiert, um zu gewährleisten, dass sofort ein Ersatz verfügbar ist, wenn ein Client die Verbindung zum Dateiserver verliert, damit eine durchgehende Verfügbarkeit der Daten gewährleistet ist.

Das Verhalten von Windows-Clients bei Ausfällen birgt ein höheres Risiko von Anwendungsunterbrechungen als andere Plattformen, da es von einer aufgebauten TCP-Transport-Verbindung abhängt. Wenn die Verbindung unterbrochen wird — wie bei einem Datei-Server-Ausfall und dessen Ersatz durch einen Failover-Server — muss eine neue Verbindung aufgebaut werden. Es ist selten, dass eine Windows-Client-Applikation so programmiert ist, dass sie sich korrekt von einer unterbrochenen Transport-Verbindung erholt. Daher werden die meisten Applikationen in irgendeiner Art unterbrochen — im schlimmsten Fall abgebrochen — und erfordern einen Neustart.

Wenn eine Client-Session Schreib- und Lese-Vorgänge mit Oplocks lokal gepuffert hat, ist es wahrscheinlich, dass die Daten verloren gehen, wenn die Applikation neu startet oder sich nach der TCP-Unterbrechung wieder verbindet. Wenn die TCP-Verbindung ausfällt, ist der Status des Clients verloren. Wenn der Server die Verbindung wiederherstellt, wird keine Aufforderung zum Brechen des Oplocks an den Client gesandt. In diesem Fall ist die Arbeit aus der vorangegangenen Session verloren. Durch die Echtzeit-Überwachung dieses Szenarios mit deaktivierten Oplocks und des Clients, der Daten auf den Datei-Server schreibt, wird

die Ausfallsicherung die Daten auf der Platte so bewahren, wie sie zum Zeitpunkt des Verbindungsabbruchs existiert haben.

In „*mission-critical*“ Hochverfügbarkeitsumgebungen sollte große Vorsicht im Umgang mit Oplocks geübt werden. Idealerweise sollten umfassende Tests mit allen betroffenen Applikationen erfolgen, sowohl mit als auch ohne aktivierte Oplocks.

13.3 Samba-Oplock-Kontrolle

Oplocks sind ein einzigartiges Datei-Sperr-Feature von Windows. Sie sind keine richtigen Dateisperren, werden aber in die meisten Diskussionen über Windows-Dateisperren miteinbezogen, also de facto als Sperr-Feature betrachtet. Oplocks sind tatsächlich ein Teil des Windows-Client-Datei-Caching-Mechanismus. Sie sind kein speziell robustes oder zuverlässiges Feature, wenn sie in der Vielzahl von angepassten Netzwerken implementiert werden, die es in Unternehmensumgebungen gibt.

Wie Windows implementiert Samba Oplocks als eine server-seitige Komponente des client-seitigen Cache-Mechanismus. Wegen des leichtgewichtigen Entwurfs des Windows-Features muss man für die effektive Konfiguration von Oplocks ihre Einschränkungen genau kennen und dieses Wissen beim Konfigurieren des Datenzugriffs für jeden einzelnen Zustand von Netzwerk- und Client-Verwendung auch anwenden.

Opportunistisches Sperren bedeutet grundsätzlich, dass es dem Client erlaubt wird, eine Datei herunterzuladen und sie lokal auf seiner Platte zu puffern, während er Veränderungen daran vornimmt; wenn ein zweiter Client auf die Datei zugreifen will, erhält der erste Client ein Signal zum Bruch des Oplocks und muss die Datei wieder zurück auf den Server synchronisieren. Dies kann in einigen Fällen deutliche Performance-Steigerungen verursachen; manche Programme bestehen nur für eine einzelne Veränderung auf der Synchronisation der gesamten Datei mit dem Server.

Level1 Oplocks (auch bekannt als einfache „*Oplocks*“) sind ein anderer Begriff für das opportunistische Sperren.

Level2 Oplocks bieten opportunistisches Sperren für eine Datei, die als *read only* behandelt wird. Dies wird typischerweise für Dateien verwendet, die read-only sind, oder für Dateien, bei denen beim Öffnen keine Absicht besteht, darauf zu schreiben.

Kernel-Oplocks sind grundsätzlich eine Methode, die es dem Linux-Kernel erlaubt, mit Sambas opportunistisch gesperrten Dateien zu koexistieren, obwohl dies eine bessere Integration von MS-Windows-Netzwerk-Dateisperren mit dem darunterliegenden Betriebssystem gebracht hat; SGI IRIX und Linux sind derzeit die einzigen oplock-fähigen Betriebssysteme.

Sie sollten Oplocks deaktivieren, wenn Sie auf dieselben Dateien sowohl von UNIX/Linux- als auch von SMB-Clients aus zugreifen, außer wenn Ihr System Kernel-Oplocks unterstützt. Unabhängig davon sollten Oplocks immer deaktiviert sein, wenn Sie eine Datenbank-Datei (z.B. Microsoft Access) für mehrere Clients freigeben, da jeder Oplock-Bruch, den der erste Client empfängt, die Synchronisation der gesamten Datei bewirkt (nicht nur des einzelnen Eintrags), was in einer merklichen Beeinträchtigung der Performance resultiert, und, noch wahrscheinlicher, in Problemen mit dem Zugriff auf die Datenbank. Bemerkenswerterweise reagieren Microsoft Outlooks persönliche Ordner (*.pst) ziemlich schlimm auf Oplocks. Im

Zweifelsfall sollten Sie Oplocks deaktivieren und Ihr System von diesem Ausgangspunkt aus einstellen.

Wenn client-seitiges Cachen in Ihrem Netzwerk erwünscht und zuverlässig ist, werden Sie vom Aktivieren der Oplocks profitieren. Wenn Ihr Netzwerk langsam und/oder unzuverlässig ist oder Sie Ihre Dateien über mehr als einen Freigabe-Mechanismus (z.B. NFS) oder ein WAN bereitstellen oder viele Anwender regelmäßig auf dieselben Dateien zugreifen, werden Sie voraussichtlich wegen des entstehenden Overheads durch das Management der Oplocks nicht von einer Aktivierung profitieren. In diesem Fall werden Sie die Oplocks stattdessen lieber deaktivieren.

Ein weiterer zu bedenkender Faktor ist die resultierende Performance des Dateizugriffs. Wenn Oplocks keinen messbaren Geschwindigkeitszuwachs in Ihrem Netzwerk bringen, macht es wahrscheinlich keinen Sinn, sich mit ihnen herumzuschlagen.

13.3.1 Beispielkonfiguration

Im folgenden Abschnitt untersuchen wir zwei verschiedene Aspekte der Samba-Sperren.

13.3.1.1 Oplocks deaktivieren

Sie können Oplocks wie folgt auf einer Pro-Freigabe-Basis deaktivieren:

```
[acctdata]
        oplocks = False
        level2 oplocks = False
```

Der Standard-Oplock-Typ ist Level1. Level2-Oplocks werden auf einer Pro-Freigabe-Basis in der Datei `smb.conf` aktiviert.

Andererseits können Sie Oplocks auf einer Pro-Datei-Basis innerhalb der Freigabe deaktivieren:

```
        veto oplock files = /*.mdb/*.MDB/*.dbf/*.DBF/
```

Wenn Sie Probleme mit Oplocks haben, die in Sambas Protokoll-Einträgen ersichtlich sind, möchten Sie vielleicht lieber auf der sicheren Seite bleiben und Oplocks und Level2-Oplocks deaktivieren.

13.3.1.2 Kernel-Oplocks deaktivieren

kernel oplocks ist ein Parameter in `smb.conf`, der Samba informiert (wenn der UNIX-Kernel die Fähigkeit hat, einem Windows-Client einen Oplock-Bruch zu senden), wenn ein UNIX-Prozess versucht, eine Datei zu öffnen, die gepuffert wird. Dieser Parameter zielt auf die gemeinsame Nutzung von Dateien zwischen UNIX und Windows mit aktivierten Oplocks auf dem Samba-Server; der UNIX-Server kann die Datei öffnen, die durch Oplocks vom Windows-Client gesperrt (= gepuffert) ist, und der smbd-Prozess sendet keinen Oplock-Bruch, der die Datei sehr wahrscheinlich zerstören würde. Wenn der UNIX-Kernel die Fähigkeit hat, einen Oplock-Bruch zu senden, dann befähigt der Parameter kernel oplocks

Samba dazu, den Oplock-Bruch zu senden. Kernel-Oplocks werden auf einer Per-Server-Basis in der Datei `smb.conf` aktiviert.

kernel oplocks = yes Die Voreinstellung ist no.

veto oplocks ist ein Parameter in `smb.conf`, der spezifische Dateien angibt, für die Oplocks deaktiviert werden. Wenn ein Windows-Client eine Datei öffnet, die mit veto oplocks konfiguriert worden ist, wird dem Client der Oplock nicht erlaubt, und alle Operationen werden auf der originalen Datei auf der Platte durchgeführt, anstatt auf der vom Client gepufferten Kopie der Datei. Durch explizites Angeben der Dateien, die mit UNIX-Prozessen geteilt werden, und durch das Deaktivieren der Oplocks für diese Dateien kann die serverweite Oplock-Konfiguration aktiviert werden, um es Windows-Clients zu erlauben, den Performance-Gewinn aus dem Datei-Caching zu nutzen, ohne das Risiko zerstörter Dateien einzugehen. Veto-Oplocks können auf einer Per-Freigabe-Basis aktiviert werden oder global für den gesamten Server. Dies erfolgt in der Datei `smb.conf` wie in Beispiel **??**.

Beispiel 13.3.1. Freigabe mit einigen Dateien mit Oplocks

```
[global]
        veto oplock files = /dateiname.htm/*.txt/

[share_name]
        veto oplock files = /*.exe/dateiname.ext/
```

oplock break wait time ist ein Parameter in `smb.conf`, der das Zeit-Intervall justiert, in dem Samba auf eine Anfrage zum Bruch eines Oplocks reagiert. Samba empfiehlt: „*Do not change this parameter unless you have read and understood the Samba oplock code.*“ oplock break wait time kann nur global in der Datei `smb.conf` konfiguriert werden, wie nachfolgend gezeigt wird:

```
        oplock break wait time = 0 (default)
```

oplock break contention limit ist ein Parameter in `smb.conf`, der die Antwort des Samba-Servers auf die Anfrage nach einem Oplock einschränkt, wenn die Anzahl der sich darum „*bewerbenden*“ Clients das in diesem Parameter angegebene Limit erreicht. Samba empfiehlt: „*Do not change this parameter unless you have read and understood the Samba oplock code.*“ *oplock break contention limit* kann auf einer Per-Freigabe-Basis aktiviert werden oder global für den gesamten Server. Dies erfolgt in der Datei `smb.conf` wie in Beispiel **??**.

Beispiel 13.3.2. Konfiguration mit oplock break contention limit

```
[global]
        oplock break contention limit = 2 (default)

[share_name]
        oplock break contention limit = 2 (default)
```

13.4 Oplock- und Cache-Kontrollen mit MS Windows

Es gibt einen bekannten Umstand beim Ausführen von Applikationen (wie Norton Anti-Virus) auf einer Windows 2000/XP-Workstation, der jede Anwendung beeinflussen kann, die versucht, über ein Netzwerk auf freigegebene Datenbank-Dateien zuzugreifen. Dies ist eine Folge einer Voreinstellung im Windows 2000/XP-Betriebssystem, dies *opportunistic locking* heißt. Wenn eine Workstation versucht, auf freigegebene Dateien auf einem anderen Windows 2000/XP-Rechner zuzugreifen, versucht das Windows 2000/XP-Betriebssystem, die Performance zu erhöhen, indem es die Dateien sperrt und lokal puffert. Wenn das passiert, kann die Anwendung nicht mehr korrekt arbeiten, und das hat zur Folge, dass die Meldung „*Access Denied*“ während der Netzwerk-Operation angezeigt wird.

Alle Windows-Betriebssysteme in der NT-Familie, die als Datenbank-Server für Dateien arbeiten können (das soll heißen, dass dort Dateien abgelegt werden, auf die von anderen Windows-PCs aus zugegriffen wird), müssen wahrscheinlich deaktivierte Oplocks haben, um das Risiko der Beschädigung von Dateien zu minimieren. Das gilt für Windows 9x/Me, Windows NT, Windows 200x und Windows XP. [1]

Wenn Sie eine Workstation der Windows NT-Familie anstatt eines Servers verwenden, müssen Sie auch darauf die Oplocks deaktivieren. Wenn Sie zum Beispiel einen PC mit dem Betriebssystem Windows NT Workstation anstatt Windows NT Server verwenden und Sie darauf Daten abgelegt haben, auf die von anderen Windows-PCs zugegriffen wird, werden Sie die Oplocks auf diesem System deaktivieren müssen.

Der hauptsächliche Unterschied ist der Ort in der Windows-Registrierung, an dem die Werte zum Deaktivieren der Oplocks eingegeben werden. Anstatt des Eintrags LanManServer muss eventuell der Eintrag LanManWorkstation verwendet werden.

Sie können diesen Wert mit dem Windows-Registrierungseditor überprüfen (auch hinzufügen oder ändern, falls nötig). Wenn Sie diesen Registrierungswert ändern, müssen Sie den PC neu starten, um sicherzustellen, dass die neue Einstellung wirksam wird.

Der Ort des Registrierungseintrags für Oplocks hat sich mit Windows 2000 geändert (gegenüber dem früheren Ort in Microsoft Windows NT).

> Anmerkung
>
>
>
> Windows 2000 akzeptiert nach wie vor den Registrierungseintrag `EnableOplocks`, der in früheren Windows-Versionen zum Deaktivieren von Oplocks verwendet wurde.

Sie können die Oplocks auch deaktivieren, indem Sie die folgenden Registrierungseinträge ändern:

```
HKEY_LOCAL_MACHINE\System\
```

[1] Microsoft hat dies im Knowledge-Base-Artikel 300216 dokumentiert.

```
CurrentControlSet\Services\MRXSmb\Parameters\

OplocksDisabled REG_DWORD 0 oder 1
Voreinstellung: 0 (nicht deaktiviert)
```

ANMERKUNG

Der Registrierungseintrag `OplocksDisabled` konfiguriert Windows-Clients in Hinblick darauf, ob sie Oplocks für enfernte (= nicht-lokale) Dateien anfordern oder nicht. Um die Oplocks zu deaktivieren, muss der Wert von `OplocksDisabled` auf 1 gesetzt sein.

```
HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Services\LanmanServer\Parameters

   EnableOplocks REG_DWORD 0 oder 1
   Voreinstellung: 1 (Aktiviert)

   EnableOpLockForceClose REG_DWORD 0 oder 1
   Voreinstellung: 0 (Deaktiviert)
```

ANMERKUNG

Der Registrierungseintrag `EnableOplocks` konfiguriert Windows-basierende Server (einschließlich Workstations, die Dateien freigeben) so, dass sie Oplocks für lokale Dateien erlauben oder nicht.

Um das Schließen von offenen Oplocks beim Schließen oder Verlassen eines Programms zu erzwingen, muss `EnableOpLockForceClose` auf 1 gesetzt sein.

Die folgende Liste illustriert die Arbeitsweise von Level2-Oplocks:

- Station 1 öffnet die Datei und fordert einen Oplock an.
- Da keine andere Station die Datei geöffnet hat, gewährt der Server der Station 1 einen exklusiven Oplock.
- Station 2 öffnet die Datei und fordert einen Oplock an.
- Da die Station 1 noch nicht auf die Datei geschrieben hat, fordert der Server die Station 1 dazu auf, den Oplock auf einen Level2-Oplock zu brechen.

- Station 1 leistet dem Folge und gibt ihre gepufferten Sperr-Informationen zurück an den Server.
- Station 1 informiert den Server, dass sie den Oplock auf einen Level2-Oplock geändert hat (alternativ dazu hätte die Station 1 auch die Datei schließen können).
- Der Server antwortet auf die offene Anfrage von Station 2 und gewährt dieser einen Level2-Oplock. Andere Stationen können ebenso die Datei öffnen und einen Level2-Oplock erhalten.
- Die Station 2 (oder irgendeine Station, die die Datei geöffnet hat) sendet eine Schreib-Anfrage per SMB. Der Server antwortet mit seiner entsprechenden „*write response*".
- Der Server fordert alle Stationen, die die Datei geöffnet haben, dazu auf, ihre Oplocks aufzubrechen, was bedeutet, dass keine Station mehr irgendwelche Oplocks auf dieser Datei gesetzt hat. Da die Workstations an diesem Punkt keinerlei gepufferte Schreibvorgänge oder Sperren haben können, brauchen sie auch nicht auf diese „*break-to-none*"-Aufforderung zu antworten; sie müssen lediglich, alle lokal gepufferten read-ahead-Daten verwerfen.

13.4.1 Workstation-Dienst-Einträge

```
\HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Services\LanmanWorkstation\Parameters

UseOpportunisticLocking   REG_DWORD   0 oder 1
Voreinstellung: 1 (Aktiviert)
```

Dies gibt an, ob der Redirektor Oplocks verwenden soll. Dieser Parameter sollte nur deaktiviert werden, um Probleme einzugrenzen.

13.4.2 Server-Dienst-Einträge

```
\HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Services\LanmanServer\Parameters

EnableOplocks   REG_DWORD   0 oder 1
Voreinstellung: 1 (Aktiviert)
```

Dies gibt an, ob der Server den Clients erlaubt, Oplocks für Dateien zu verwenden.

```
MinLinkThroughput   REG_DWORD   0 bis zu unendlich vielen Bytes/Sekunde
Voreinstellung: 0
```

Dies gibt den minimalen Durchsatz an, der vom Server erlaubt wird, bevor er raw-locks und Oplocks für diese Verbindung deaktiviert.

```
MaxLinkDelay   REG_DWORD   0 bis 100,000 Sekunden
Voreinstellung: 60
```

Dies gibt das zeitliche Limit für die Verzögerungen in einer Verbindung an. Wenn die Verzögerungen diesen Wert übersteigen, deaktiviert der Server raw-locks und Oplocks für diese Verbindung.

```
OplockBreakWait   REG_DWORD   10 bis 180 Sekunden
Voreinstellung: 35
```

Dies gibt die Zeit an, die der Server einem Client gibt, um auf eine Anfrage bezüglich eines Oplock-Breaks zu antworten. Kleinere Werte können helfen, abgestürzte Clients schneller zu finden, verursachen aber auch leichter den Verlust gepufferter Daten.

13.5 Andauernder Datenverlust

Wenn Sie alle in diesem Kapitel erwähnten Einstellungen gesetzt haben, aber nach wie vor Datenverluste erleiden, gibt es hier noch ein paar weitere Dinge, die Sie sich ansehen sollten.

Wir haben zuverlässige Berichte von Entwicklern, dass fehlerhafte Netzwerk-Hardware, wie eine einzelne fehlerhafte Netzwerkkarte, Symptome wie Caching-Probleme und Datenverlust verursachen kann. Wenn Sie auch nach wiederholtem Neu-Indizieren immer noch Datenverluste erleiden, müssen Sie wahrscheinlich die betreffenden Dateien neu aufbauen. Das bedeutet das Anlegen einer neuen Datei mit derselben Definition wie die neu zu bildende Datei und das Transferieren der Daten aus der alten in die neue Datei. Es gibt einige bekannte Methoden, dies zu tun, die Sie in unserer Knowledge Base finden können.

13.6 Häufige Fehler

In manchen Installationen zeigen sich Probleme mit dem Sperren, sobald ein Server installiert wird; in anderen bleiben diese Probleme für eine lange Zeit verborgen. Fast ohne Ausnahme verursachen diese Probleme Ärger und potenzielle Datenverluste.

Über die letzten paar Jahre gab es eine Anzahl von Beschwerden in der Samba-Mailing-Liste, in denen behauptet wurde, dass Samba Datenverluste verursacht habe. Drei Ursachen wurden bislang festgestellt:

- Fehlerhafte Konfiguration der Oplocks (inkompatibel mit der verwendeten Applikation). Dies ist ein gängiges Problem, sogar dort, wo MS Windows NT4- oder MS Windows 200x-basierende Server im Einsatz sind. Es ist zwingend erforderlich, dass die Anweisungen des Software-Herstellers in Bezug auf die Konfiguration der Dateisperren befolgt werden. Falls Sie im Zweifel sind, deaktivieren Sie die Oplocks sowohl auf dem

Server als auch auf dem Client. Das Deaktivieren jeglicher Form der Datei-Pufferung auf den MS Windows-Clients kann ebenso erforderlich sein.

- Defekte Netzwerk-Karten, -Kabel oder -HUBs/Switches. Dies ist im Allgemeinen eher beim Einsatz billiger Netzwerk-Hardware verbreitet, obwohl es manchmal auch Probleme mit Inkompatibilitäten bei eher teurer Hardware gibt.
- Es hat auch einzelne Meldungen gegeben, in denen berichtet wurde, dass Sambas Protokoll-Dateien über Daten-Dateien geschrieben wurden. Dies wurde nur von sehr wenigen Installationen berichtet (ungefähr fünf in den letzten drei Jahren), und alle Versuche, dieses Problem zu reproduzieren, schlugen fehl. Das Samba-Team war bislang nicht imstande, dieses Ereignis zu beobachten, und konnte daher auch noch keine spezielle Ursache eingrenzen. Bedenkt man die Millionen von Systemen, die Samba einsetzen, ist es trotzdem für die paar Administratoren, die von diesem Problem betroffen wurden, genauso wie für das Samba-Team, eine frustrierende und ärgerliche Herausforderung. Wenn Sie so etwas beobachten, erstellen Sie bitte unverzüglich einen Bug-Report auf Samba Bugzilla <`https://bugzilla.samba.org`>. Geben Sie bitte so viele Informationen wie möglich, da Sie vielleicht dazu beitragen, die Ursache dieses Problems zu isolieren und die Reproduktion des Problems zu ermöglichen (ein Schritt von grundlegender Bedeutung, um das Problem eingrenzen und beheben zu können).

13.6.1 Fehlermeldungen bezüglich locking.tdb

„*Wir haben viele Fehler in den Samba-Logs, wie:*

```
tdb(/usr/local/samba_2.2.7/var/locks/locking.tdb): rec_read bad magic
 0x4d6f4b61 at offset=36116
```

Was bedeuten diese Meldungen?“

Dieser Fehler deutet auf eine zerstörte tdb-Datei hin. Stoppen Sie alle Instanzen von smbd, löschen Sie die Datei locking.tdb, und starten Sie smbd neu.

13.6.2 Probleme beim Speichern von Dateien in MS Office auf Windows XP

Dies ist ein Bug in Windows XP. Sie finden mehr Infos dazu im Microsoft Knowledge-Base-Artikel 812937. <`http://support.microsoft.com/?id=812937`>

13.6.3 Lange Verzögerungen beim Löschen von Dateien über das Netzwerk mit XP SP1

„*Manchmal dauert es ca. 35 Sekunden, um Dateien über das Netzwerk zu löschen, nachdem XP SP1 eingespielt wurde.*“

Dies ist ein Bug in Windows XP. Sie finden mehr Infos dazu im Microsoft Knowledge-Base-Artikel 811492. <`http://support.microsoft.com/?id=811492`>

13.7 Weiterer Lesestoff

Sie möchten vielleicht auf unserer Website von Zeit zu Zeit nach einer aktualisierten Version dieser Informationen schauen. Viele der von uns zur Verfügung gestellten Hinweisen werden aktualisiert, sobald sich neue Informationen ergeben. Auf diesen „*papers*“ finden Sie das Datum der letzten Bearbeitung immer am Beginn des jeweiligen Artikels.

Der Abschnitt der Microsoft MSDN Library zum opportunistischen Sperren:

Opportunistic Locks, Microsoft Developer Network (MSDN), Windows Development > Windows Base Services > Files and I/O > SDK Documentation > File Storage > File Systems > About File Systems > Opportunistic Locks, Microsoft Corporation. <`http://msdn.microsoft.com/library/en-us/fileio/storage_5yk3.asp`>

Microsoft Knowledge-Base-Artikel Q224992 „*Maintaining Transactional Integrity with OPLOCKS*“, Microsoft Corporation, April 1999, <`http://support.microsoft.com/default.aspx?scid=kb;en-us;Q224992`>.

Microsoft Knowledge-Base-Artikel Q296264 „*Configuring Opportunistic Locking in Windows 2000*“, Microsoft Corporation, April 2001, <`http://support.microsoft.com/default.aspx?scid=kb;en-us;Q296264`>.

Microsoft Knowledge-Base-Artikel Q129202 „*PC Ext: Explanation of Opportunistic Locking on Windows NT*“, Microsoft Corporation, April 1995, <`http://support.microsoft.com/default.aspx?scid=kb;en-us;Q129202`>.

Kapitel 14

SAMBA ABSICHERN

14.1 Einführung

Diese Anmerkung wurde zu den Release-Notes zu Samba 2.2.8 hinzugefügt, da sie eine wichtige Sicherheitskorrektur enthält. Die hier enthaltene Information gilt generell für Samba-Installationen.

> Ein neuer Lehrling meldete sich beim Chef-Ingenieur eines Kesselhauses zur Arbeit. Er sagte: „*Hier bin ich, wenn Sie mir den Boiler zeigen, werde ich daran zu arbeiten beginnen.*“ Der Ingenieur antwortete:„*Du lehnst daran!*“

Sicherheitsbedenken sind genau so. Sie müssen ein wenig über das Thema wissen, um anzuerkennen, wie offensichtlich das meiste davon ist. Die Herausforderung für die meisten von uns ist, den ersten Brocken des Wissens zu entdecken, mit dem wir die Geheimnisse der Meister entschlüsseln können.

14.2 Eigenschaften und Vorzüge

Es gibt drei Ebenen, auf denen Sicherheitsprinzipien beachtet werden müssen, um eine Installation zumindest einigermaßen sicher zu gestalten. Diese sind die umgebende Firewall, die Konfiguration des Host-Servers, der Samba ausführt, und Samba selbst.

Samba erlaubt einen höchst flexiblen Ansatz zur Netzwerk-Sicherheit. Samba implementiert so weit wie möglich die neuesten Protokolle, um sicherere MS-Windows-Datei- und Druck-Operationen zu ermöglichen.

Samba kann gegenüber Verbindungen abgesichert werden, die von außerhalb des LAN herrühren. Dies kann durch die Verwendung von *host-based protection* geschehen (unter Verwendung der Samba-Implementation einer Technologie namens „*tcpwrappers*“) oder durch die Verwendung von *interface-based exclusion*, so dass smbd sich nur an bestimmte erlaubte Netz-Interfaces bindet. Es ist auch möglich, Ausschlüsse spezifisch für Freigaben oder Ressourcen zu setzen, zum Beispiel für die automatische Freigabe `[IPC$]`. Diese Freigabe wird für Browsing-Zwecke ebenso verwendet wie zur Herstellung von TCP/IP-Verbindungen.

Eine andere Methode, um Samba abzusichern, ist das Setzen von „*Access Control Entries*“

(ACEs) in einer Zugriffskontroll-Liste (ACL) auf den Freigaben selbst. Dies wird in Kapitel **??** „Zugriffskontrollen für Dateien, Verzeichnisse und Netzwerk-Freigaben“ beschrieben.

14.3 Technische Beschreibung von Schutzmaßnahmen

Die eigentliche Herausforderung bei allen Sicherheitsbestrebungen ist die Tatsache, dass Schutzmaßnahmen nur dazu ausreichen, die Tür für bekannte „*exploit*“- und „*breach*“-Techniken zu schließen. Nehmen Sie niemals an, dass der Samba-Server nun eine uneinnehmbare Festung sei, nur weil Sie ein paar Maßnahmen befolgt haben! Wenn man die bisherige Geschichte von Informationssystemen anschaut, ist es nur eine Frage der Zeit, bis jemand einen weiteren Schwachpunkt findet.

14.3.1 Host-basierter Schutz

In vielen Installationen von Samba kommt die größte Bedrohung von außerhalb des unmittelbaren Netzes. Standardmäßig akzeptiert Samba Verbindungen von jedem Host, was bedeutet, dass Sie besonders gefährdet sein können, wenn Sie eine unsichere Version von Samba auf einem Host ausführen, der direkte Verbindung zum Internet hat.

Eine der einfachsten Abhilfen in diesem Fall ist die Verwendung der Optionen hosts allow und hosts deny in der Konfigurationsdatei `smb.conf`, um den Zugriff auf Ihren Server auf eine spezifizierte Menge von Hosts einzuschränken. Ein Beispiel könnte sein:

```
hosts allow = 127.0.0.1 192.168.2.0/24 192.168.3.0/24
hosts deny = 0.0.0.0/0
```

Diese Einstellung wird nur SMB-Verbindungen von `localhost` (Ihrem eigenen Rechner) und von den beiden privaten Netzen 192.168.2 und 192.168.3 erlauben. Alle anderen Verbindungen werden abgelehnt, sobald der Client sein erstes Paket sendet. Die Ablehnung wird als not listening on called name-Fehler gekennzeichnet.

14.3.2 Benutzer-basierter Schutz

Wenn Sie den Zugriff auf Ihren Server nur auf gültige Benutzer beschränken wollen, kann folgende Methode von Nutzen sein. Im Abschnitt *[global]* der Datei `smb.conf` setzen Sie:

```
valid users = @smbusers, jacko
```

Dies schränkt allen Server-Zugriff auf entweder den Benutzer *jacko* oder Mitglieder der System-Gruppe *smbusers* ein.

14.3.3 Benutzen von Schnittstellen-Schutz

Standardmäßig akzeptiert Samba Verbindungen auf jeder Netzwerk-Schnittstelle, die es in Ihrem System findet. Das bedeutet: Wenn Sie eine ISDN-Verbindung oder einen PPP-Tunnel zum Internet haben, wird Samba Verbindungen über diese Schnittstellen akzeptieren. Das könnte etwas sein, das Sie nicht wollen.

Sie können dieses Verhalten ändern:

```
interfaces = eth* lo
bind interfaces only = yes
```

Dies weist Samba an, Verbindungen nur auf Schnittstellen zu erwarten, die mit `eth` beginnen (wie `eth0, eth1`) sowie auf dem loopback-Interface namens `lo`. Der zu verwendende Name hängt vom verwendeten Betriebssystem ab. Im Beispiel oben wurden die unter Linux gängigen Namen für Ethernet-Karten verwendet.

Wenn Sie das obige Beispiel verwenden und jemand versucht, eine SMB-Verbindung über eine PPP-Schnittstelle namens `ppp0` herzustellen, wird er eine Ablehnung erhalten. In diesem Fall wird keinerlei Samba-Code ausgeführt, da das OS angewiesen wurde, keine Verbindungen von dieser Schnittstelle an irgendeinen Samba-Prozess weiterzuleiten.

14.3.4 Verwendung einer Firewall

Viele verwenden eine Firewall, um Zugriff auf Dienste zu sperren, die sie nicht außerhalb ihres Netzwerks anbieten wollen. Dies kann eine gute Idee sein, obwohl wir empfehlen, die Firewall gemeinsam mit obigen Methoden einzusetzen, so dass Sie auch geschützt sind, wenn die Firewall aus irgendwelchen Gründen nicht aktiv ist.

Wenn Sie eine Firewall aufsetzen, müssen Sie wissen, welche TCP- und UDP-Ports zu öffnen bzw. zu blockieren sind. Samba benutzt die folgenden Ports:

UDP/137 - verwendet von nmbd
UDP/138 - verwendet von nmbd
TCP/139 - verwendet von smbd
TCP/445 - verwendet von smbd

Der letzte Port ist wichtig, da ihn viele ältere Firewall-Setups möglicherweise nicht berücksichtigen, weil dieser Port erst in den letzten Jahren zum Protokoll hinzugefügt wurde.

14.3.5 Verwenden von Ablehnungen, die auf IPC$-Freigaben basieren

Wenn die obigen Methoden nicht anwendbar sind, könnten Sie auch eine spezifischere Ablehnung auf der IPC$-Freigabe setzen, die in einer kürzlich entdeckten Sicherheitslücke verwendet wird. Dies erlaubt Ihnen, Zugriff auf andere Freigaben anzubieten, während Sie den Zugriff von potenziell nicht vertrauenswürdigen Hosts auf IPC$ ablehnen.

Um dies zu tun, verwenden Sie folgendes:

```
[IPC$]
        hosts allow = 192.168.115.0/24 127.0.0.1
        hosts deny = 0.0.0.0/0
```

Dies weist Samba an, dass IPC$-Verbindungen nicht erlaubt sind, außer von den zwei angeführten Netzwerk-Adressen (localhost und dem Subnetz 192.168.115). Verbindungen zu anderen Freigaben sind weiter erlaubt. Da die IPC$-Freigabe die einzige Freigabe ist, auf die anonym zugegriffen werden kann, schafft dies einen gewisse Schutz vor Angreifern, die keine gültige Benutzernamen/Passwort-Kombination für Ihren Server kennen.

Wenn Sie diese Methode anwenden, werden Clients eine 'access denied'-Meldung erhalten, wenn sie versuchen, sich mit der IPC$-Freigabe zu verbinden. Diese Clients werden keine Freigaben durchsuchen können, und sie können auch manche andere Dienste nicht benutzen. Diese Methode wird nicht empfohlen, außer Sie können aus einem bestimmten Grund keine der anderen oben beschriebenen Methoden anwenden.

14.3.6 NTLMv2-Sicherheit

Um eine NTLMv2-Authentifizierung zu konfigurieren, sind die folgenden Registrierungsschlüssel wichtig:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"lmcompatibilitylevel"=dword:00000003
```

Der Wert 0x00000003 bedeutet, dass nur NTLMv2-Antworten gesendet werden. Clients werden die NTLMv2-Authentifizierung verwenden, und die NTLMv2-Session-Security, wenn es der Server unterstützt. Domänencontroller akzeptieren LM-, NTLM- und NTLMv2-Authentifizierung.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0]
"NtlmMinClientSec"=dword:00080000
```

Der Wert 0x00080000 bedeutet, dass nur NTLMv2-Session-Security akzeptiert wird. Wenn entweder NtlmMinClientSec oder NtlmMinServerSec auf 0x00080000 gesetzt ist, wird die Verbindung fehlschlagen, wenn die NTLMv2-Session-Security nicht ausgehandelt wird.

14.4 Upgrade von Samba

Bitte überprüfen Sie regelmäßig <`http://www.samba.org/`> auf Updates und wichtige Verlautbarungen. Gelegentlich werden Sicherheits-Releases herausgegeben, und wir empfehlen Ihnen dringend, ein Upgrade von Samba durchzuführen, wenn eine Sicherheitslücke entdeckt wird. Prüfen Sie auch die Seiten des Lieferanten Ihres Betriebssystems auf Upgrades, die spezifisch für Ihr Betriebssystem sind.

14.5 Häufige Fehler

Wenn die ganze Konfiguration von Samba und seiner Host-Plattform wirklich so intuitiv wäre, wie es sich mancher wünscht, dann wäre dieser Abschnitt unnötig. Sicherheitsfragen sind oft ärgerlich für die Support-Person, die sie zu lösen hat, nicht nur wegen der Komplexität des Problems, sondern aus dem Grunde, dass die meisten Administratoren, die von etwas berichten, das sich dann als Sicherheitsproblem herausstellt, völlig überzeugt davon sind, dass das Problem an Samba liegt.

14.5.1 Smbclient funktioniert auf Localhost, aber das Netzwerk ist tot

Das ist ein verbreitetes Problem. Red Hat Linux (und andere) installiert eine Firewall. Mit der Standard-Firewall wird nur Verkehr auf dem loopback-Adapter (IP 127.0.0.1) durch die Firewall gelassen.

Die Lösung ist es, entweder die Firewall zu entfernen (stoppen) oder das Firewall-Skript so zu modifizieren, dass die Firewall SMB-Netzwerk-Verkehr durchlässt (siehe den obigen Abschnitt hierzu).

14.5.2 Warum können Benutzer auf die home-Verzeichnisse anderer Benutzer zugreifen?

„*We are unable to keep individual users from mapping to any other user's home directory once they have supplied a valid password! They only need to enter their own password. I have not found any method to configure Samba so that users may map only their own home directory.(((Bitte übersetzen)))*“

„*User xyzzy can map his home directory. Once mapped user xyzzy can also map anyone else's home directory.(((Bitte übersetzen)))*“

Dies ist kein Sicherheitsversäumnis, sondern vom Design so vorgesehen. Samba erlaubt Benutzern denselben Zugriff auf das UNIX-Dateisystem, als wären sie an der UNIX-Maschine angemeldet, mit der Einschränkung, dass es nur Zugriff auf die Dateien erlaubt, die von den definierten Freigaben erlaubt sind.

Wenn Ihre UNIX-home-Verzeichnisse so angelegt sind, dass ein Benutzer einfach per **cd** in das home-Verzeichnis eines anderen Benutzers gelangen und **ls** ausführen kann, so ist die UNIX-Sicherheitslösung dafür, die Datei-Erlaubnisse für die home-Verzeichnisse so zu setzen, dass die Befehle **cd** und **ls** abgelehnt werden.

Samba ist so eingeichtet, dass es die Sicherheitsrichtlinien des UNIX-Administrators nicht hinterfragt und ihm zu vertraut, dass er die Richtlinien und Erlaubnisse so setzt, wie er es für richtig hält.

Samba erlaubt das gewünschte Verhalten. Setzen Sie einfach die Option only user = %S im Abschnitt der *[homes]*-Freigaben-Definition.

Die Option only user arbeitet in Wechselwirkung mit users = list, also müssen Sie, um das gewünschte Verhalten zu erzielen, folgende Zeile hinzufügen: *users = %S* Dies ist gleichbedeutend zum Hinzufügen von *valid users = %S* zur Definition der *[homes]*-Freigabe, wie es in der Manpage zu `smb.conf` empfohlen wird.

Kapitel 15

INTERDOMAIN-VERTRAUENSSTELLUNGEN

Samba-3 unterstützt NT4-gleiche Domänen-Vertrauensstellungen. Dies ist eine Eigenschaft, die viele Sites benutzen möchten, wenn sie von einer NT4-gleichen Domäne auf eine Samba-3-Domäne migrieren, aber kein Active Directory oder ein LDAP-basierendes Backend übernehmen möchten. Dieses Kapitel beschreibt einige Hintergrundinformationen zu Vertrauensstellungen und zeigt, wie sie erstellt werden. Samba-3 kann jetzt NT4 vertrauen (und umgekehrt), genauso wie es möglich ist, Samba-zu-Samba-Vertrauensstellungen zu erstellen.

15.1 Eigenschaften und Vorzüge

Samba-3 kann an einer Samba-zu-Samba-Vertrauensstellung teilnehmen, genauso wie an einer Samba -zu-MS-Windows-NT4-Vertrauensstellung. Somit hat Samba eine ähnliche Skalierbarkeit wie MS Windows NT4.

Da Samba-3 die Fähigkeit besitzt, mit einem skalierbaren Authentifizierungsbackend wie LDAP zu funktionieren, und es sowohl als primärer Domänencontroller als auch als Backup-Domänencontroller funktioniert, sollte der Administrator sich nach Alternativen umschauen, bevor er die Interdomänen-Vertrauensstellung benutzt, aus dem einfachen Grund, dass das Prinzip, nach dem sie arbeiten, einfach unsicher ist. Dies war, unter anderem, ein Hauptgrund für die Entwicklung von Microsoft Active Directory.

15.2 Hintergrund von Vertrauensstellungen

MS Windows NT3/4-Sicherheitsdomänen haben eine nicht-hierarchische Sicherheitsstruktur. Die Einschränkungen dieser Architektur und die Tatsache, wie sie die Skalierbarkeit von MS Windows- Netzwerken in großen Organisationen betreffen, sind wohl bekannt. Dazu schränkt der flache Namensraum, der aus diesem Design resultiert, auch die Verteilung von administrativen Aufgaben in großen Netzwerken sehr ein.

Microsoft entwickelte Active Directory Service (ADS), das auf Kerberos und LDAP basiert, um die Einschränkungen der älteren Technologien zu umgehen. Nicht jede Organisation

ist gewillt oder bereit, ADS einzusetzen. Für kleinere Unternehmen ist das alte NT4-Domänensicherheitsmuster eher angebracht; es bleibt eine feste Benutzerbasis, für die es keinen Grund gibt, eine mit Betriebsunterbrechungen einhergehende Umstellung der Technologie durchzuführen, um ADS zu adaptieren.

Mit MS Windows NT hat Microsoft die Fähigkeit eingeführt, unterschiedlichen Sicherheitsdomänen einen Mechanismus zu erlauben, mit dem Benutzern einer Domäne Anmelderechte und Privilegien in einer anderen Domäne gegeben werden können. Dies wird als *Vertrauensstellung* (Trust) bezeichnet. So *vertraut* beispielsweise eine Domäne den Benutzern einer anderen Domäne. Die Domäne, deren Benutzer einer anderen Domäne zur Verfügung stehen, nennt man vertraute Domäne. Die Domäne, in der diese Benutzer gewisse Rechte und Privilegien haben, ist die vertrauende Domäne. Mit NT3.x/4.0 gehen alle Vertrauensstellungen immer nur in eine Richtung, d.h., wenn Benutzer beider Domänen in der jeweils anderen Domäne Rechte und Privilegien haben sollen, muss man zwei Vertrauensstellungen aufbauen: eine in jede Richtung.

In einer NT4-artigen MS-Sicherheitsdomäne sind alle Vertrauensstellungen nicht-transitiv. Das bedeutet: Wenn wir drei Domänen haben (nennen wir sie ROT, WEISS und BLAU), in der ROT und WEISS in einer Vertrauensstellung zueinander stehen und WEISS und BLAU in einer Vertrauensstellung zueinander stehen, dann bedeutet das nicht, dass ROT und BLAU automatisch eine Vertrauensstellung zueinander haben. Vertrauensstellungen sind explizit und nicht transitiv.

Neu im MS Windows 2000-ADS-Sicherheitskontext ist die Tatsache, dass Vertrauensstellungen per Voreinstellung in beiden Richtungen verlaufen. Zusätzlich sind alle Inter-ADS-Domänen-Vertrauensstellungen transitiv. Im Fall der Domänen ROT, WEISS und BLAU und Windows 2000 mit ADS würde das bedeuten, dass ROT und BLAU sich vertrauen würden. Dies ist eine Eigenschaft, die nur ADS-Domänen haben. Samba-3 implementiert MS Windows NT4-artige Domänen-Vertrauensstellungen und verkehrt mit MS Windows 200x-ADS-Sicherheitsdomänen in einer ähnlichen Weise wie mit MS Windows NT4-artigen Domänen.

15.3 Native MS Windows NT4-Vertrauenstellungen konfigurieren

Zwei Schritte sind erforderlich, um eine Interdomain-Vertrauensstellung herzustellen. Um eine 2-Wege-Vertrauensstellung aufzubauen, müssen beide Domänenadministratoren einen Trust Account für die jeweils andere Domäne anlegen, der dazu dient, die Sicherheitsbeschränkungen zu überprüfen.

15.3.1 Eine NT4-Vertrauensstellung aufbauen

In MS Windows NT4 werden alle Domänen-Vertrauensstellungen mit dem Domain User Manager konfiguriert. Sie rufen ihn über den Eintrag **Domain User Manager Policies** in der Menüleiste auf. Vom **Policy**-Menü aus wählen Sie **Trust Relationships**. Gleich neben der unteren Box mit dem Namen **Permitted to Trust this Domain** sind zwei Buttons, **Add** und **Remove**. Der **Add**-Button öffnet ein Menü, in dem man den Namen der Domäne eintragen kann, die dann befähigt ist, Zugriffsrechte an Benutzer in Ihrer Domäne zu vergeben. Sie müssen auch ein Passwort für diese Vertrauensstellung eingeben, das die

vertrauende Domäne benötigt, wenn sie Benutzer aus der vertrauten Domäne authentifiziert. Das Passwort muss zweimal eingegeben werden (Standard-Bestätigung).

15.3.2 Eine NT4-Vertrauensstellung fertig stellen

Eine Vertrauensstellung funktioniert nur, wenn die andere (vertrauende) Domäne die benötigten Verbindungen mit der vertrauten Domäne herstellt. Um das Vertrauensverhältnis herzustellen, muss der Administrator den Domain User Manager starten, dann unter **Policies** den Menüpunkt **Trust Relationships** auswählen und auf den **Add**-Button klicken, der sich neben der **Trusted Domains**-Box befindet. Es öffnet sich ein Menü, in dem man den Namen der anderen Domäne sowie das Passwort zur Vertrauensstellung eingeben muss.

15.3.3 Interdomain-Vertrauensmöglichkeiten

Eine 2-Wege-Vertrauensstellung ist erstellt, wenn zwei Einweg-Vertrauensstellungen erstellt worden sind, und zwar eine in jede Richtung. Wo eine Einweg-Vertrauensstellung zwischen zwei MS Windows NT4-Domänen besteht (nennen wir sie DomA und DomB), wurden folgende Möglichkeiten hergestellt:

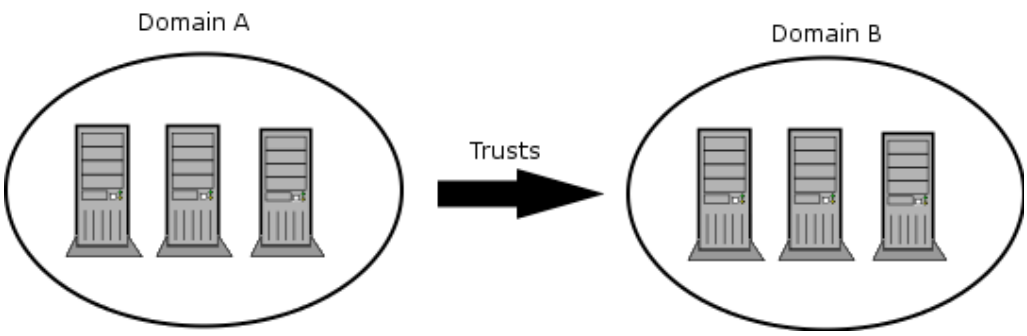


Figure 15.1. Überblick über Vertrauensstellungen

- DomA (stellt die Vertrauensverbindung fertig) *vertraut* DomB.
- DomA ist die *vertrauende* Domäne.
- DomB ist die *vertraute* Domäne (initiiert die Vertrauensstellung).
- Benutzer aus DomB können auf Ressourcen aus DomA zugreifen.
- Benutzer aus DomA können nicht auf Ressourcen aus DomB zugreifen.
- Globale Grppen aus DomB können in DomA benutzt werden.
- Globale Gruppen aus DomA können nicht in DomB benutzt werden.
- DomB erscheint im Logon-Dialog auf Client-Workstations von DomA.
- DomA erscheint nicht im Logon-Dialog auf Client-Workstations von DomB.

- Den Benutzern/Gruppen in einer vertrauenden Domäne können keine Zugriffe oder Rechte zu einer vertrauten Domäne gegeben werden.
- Die vertrauende Domäne kann auf Konten (Benutzer/globale Gruppen) der vertrauten Domäne zugreifen und sie benutzen.
- Den Administratoren der vertrauten Domäne können administrative Rechte in der vertrauenden Domäne gegeben werden.
- Den Benutzern in einer vertrauten Domäne können Rechte und Privilegien in der vertrauenden Domäne gegeben werden.
- Den globalen Gruppen der vertrauten Domäne können Rechte und Zugriffe in der vertrauenden Domäne gegeben werden.
- Globale Gruppen einer vertrauten Domäne können Mitglieder in den lokalen Gruppen einer Maschine werden, die Mitglied einer MS Windows-Domäne ist.

15.4 Konfigurieren einer NT-artigen Vertrauensstellung mit Samba

Diese Beschreibung ist eine recht kurze Einführung sein, wie man einen Samba-Server so aufsetzt, dass er an einer Inderdomain-Vertrauensstellung teilnehmen kann. Die Unterstützung von Verstrauensstellungen in Samba befindet sich in einem frühen Stadium, deshalb sollten Sie nicht überrascht sein, wenn etwas nicht so funktioniert, wie es sollte.

Alle unten beschriebenen Szenarien gehen davon aus, dass die Peer-Domäne in der Vertrauensstellung von einem Windows NT4-Server betrieben wird. Das entfernte Ende könnte aber auch genauso gut eine andere Samba-3-Domäne sein. Nachdem Sie dieses Dokument zu Ende gelesen haben, werden Sie erkennen, dass man, wenn man die Samba-spezifische Teile der folgenden Anleitungen zusammensetzt, auch eine Vertrauensstellung zwischen Domänen in einer reinen Samba-Umgebung herstellen kann.

15.4.1 Samba als vertraute Domäne

Um den Samba-PDC als vertraute Seite der Vertrauensstellung festzulegen, muss zuerst ein spezielles Konto in der Domäne erstellt werden, die die vertrauende Seite sein wird. Dazu verwenden Sie das Programm **smbpasswd**. Ein vertrautes Domänen-Konto zu erstellen funktioniert ähnlich, wie ein vertrautes Maschinen-Konto zu erstellen. Nehmen wir an, Ihre Domäne heißt SAMBA und die entfernte Domäne ist RUMBA. Der erste Schritt ist, folgenden Befehl in Ihrer Lieblings-Shell auszuführen:

```
root#  smbpasswd -a -i rumba
New SMB password: XXXXXXXX
Retype SMB password: XXXXXXXX
Added user rumba$
```

Dabei bedeutet `-a`, dass ein neues Konto zur passdb-Datenbank hinzugefügt wird, und `-i` heißt so viel wie: „*Erstelle dieses Konto mit dem Interdomain-Vertrauens-Flag*“.

Der Kontoname lautet nun „*rumba$*“ (das ist der Name der entfernten Domäne). Falls dies fehlschlägt, sollten Sie überprüfen, ob das Konto zur System-Password-Datenbank (`/etc/passwd`) hinzugefügt wurde. Falls nicht, können sie es von Hand hinzufügen und dann den obigen Schritt wiederholen.

Nachdem Sie diesen Befehl eingegeben haben, werden Sie nach einem Passwort für dieses Konto gefragt. Sie können hier jedes beliebige Passwort verwenden, aber beachten Sie, dass Windows NT dieses Passwort nicht früher als 7 Tage nach der Konto-Erstellung ändern wird. Nach erfolgreicher Ausführung des Befehls können Sie den Eintrag für das neue Konto anschauen (in der Art, die Ihre Konfiguration vorsieht), und Sie werden sehen, dass der Kontoname wirklich RUMBA$ ist und dass das „*I*“-Flag im flags-Feld gesetzt ist. Sie können nun die Vertrauensstellung bestätigen, indem Sie sie vom Windows NT-Server aus aufbauen.

Öffnen Sie den User Manager for Domains, und wählen Sie im **Policies**-Menü den Eintrag **Trust Relationships...**. Neben der **Trusted domains**-Listbox klicken Sie auf den **Add...**-Button. Sie werden nach dem Namen der vertrauten Domäne und dem dazugehörigen Passwort gefragt. Geben Sie SAMBA an, da dies der Name unserer entfernten Domäne ist, und das Passwort das bei der Konto-Erstellung verwendet wurde. Klicken Sie auf **OK**, und wenn alles ohne Fehler funktioniert hat, werden Sie die Mitteilung `Trusted domain relationship successfully established` bekommen.

15.4.2 Samba als die vertrauende Domäne

Jetzt werden die Aufgaben umgekehrt. Wieder nehmen wir an, dass Ihre vom Samba-PDC kontrollierte Domäne SAMBA heißt und die NT-kontrollierte Domäne RUMBA.

Der erste Schritt besteht darin, ein Konto für die SAMBA-Domäne auf dem PDC RUMBA zu erstellen.

Starten Sie den Domain User Manager, und wählen Sie im Menü **Policies** den Eintrag **Trust Relationships** aus. Jetzt klicken Sie auf den **Add**-Button, der sich neben der **Trusted Domains**-Box befindet, und geben den Namen der vertrauten Domäne (SAMBA) und das Passwort für die Sicherung der Vertrauensstellung ein.

Das Passwort kann willkürlich gewählt werden. Es ist einfach, das Passwort zu jedem Zeitpunkt vom Samba-Server aus zu ändern. Nachdem man das Passwort bestätigt hat, ist das Konto fertig für den Gebrauch. Jetzt ist der Samba-Server an der Reihe.

Sie melden sich mit ihrer bevorzugten Shell als root an und führen folgenden Befehl aus:

```
root#net rpc trustdom establish rumba
```

Sie werden nach dem Passwort gefragt, das Sie gerade in Ihrer Windows NT4-Server-Maschine eingegeben haben. Die Fehlermeldung ‘NT_STATUS_NOLOGON_INTERDOMAIN_TRUST_A
die manchmal auftritt, kann getrost ignoriert werden. Sie bedeutet, dass das Passwort, das Sie eingegeben haben, richtig ist, und der NT4-Server sagt damit, dass das Konto für eine Interdomain-Verbindung zur Verfügung sthet und nicht für eine normale Verbindung. Nach dieser Prozedur müssen Sie etwas gedulding sein, es könnte eine Weile dauern (vor allem in großen Netzwerken), aber schließlich sollten Sie die `Success`-Meldung sehen. Gratulation! Ihre Vertrauensstellung wurde in diesem Moment fertig gestellt.

ANMERKUNG

Sie müssen diesen Befehl als root ausführen da sie Schreibrechte auf die Datei `secrets.tdb` haben müssen.

15.5 NT4-artie Domänen-Vertrauensstellungen mit Windows 2000

Obwohl der Domain User Manager unter Windows 2000 nicht mehr existiert, ist es trotzdem möglich, eine NT4-artige Vertrauensstellung mit einem Windows 2000-Domänencontroller, der im gemischten Modus als vertrauender Server läuft, aufzubauen. Es sollte auch für Samba möglich sein, einem Windows 2000-Server zu vertrauen, in diesem Gebiet muss jedoch noch getestet werden.

Nachdem Sie ein Interdomain-Vertrauenskonto auf dem Samba-Server wie oben beschrieben erstellt haben, öffnen Sie Active Directory Domains and Trusts auf dem AD-Controller der Domäne, deren Ressourcen Sie den Samba-Benutzern zur Verfügung stellen möchten. Wenn Sie möchten, dass Ihre Benutzer Zugriff auf mehrere Mixed-Mode-Domänen in Ihrem AD-Forest haben, müssen Sie diesen Vorgang für alle Domänen wiederholen. Nachdem Sie Active Directory Domains and Trusts geöffnet haben, machen Sie einen Rechtsklick auf die Domäne, die Ihrer Samba-Domäne vertrauen soll, und wählen **Properties**. Dann klicken Sie auf den **Trusts**-Tab. Im oberen Teil der Leiste sehen Sie eine Listbox mit dem Namen **Domains trusted by this domain:** und einem **Add...**-Button daneben. Drücken Sie diesen Knopf, und wie bei NT4 werden Sie nun nach der Domäne und dem Passwort für die Vertrauensstellung gefragt. Klicken Sie auf OK, und nach einem Moment wird Active Directory mit der Meldung `The trusted domain has been added and the trust has been verified.` antworten. Ihren Samba-Benutzern kann nun Zugriff auf die Ressourcen in der AD-Domäne gegeben werden.

15.6 Häufige Fehler

Interdomain-Vertrauensstellungen sollten nicht in Netzwerken erstellt werden, die instabil sind oder öfter Ausfälle haben. Netzwerkstabilität und -integrität sind Schlüsselvoraussetzungen für verteilte vertraute Domänen.

15.6.1 Das Durchsuchen der vertrauten Domäne schlägt fehl

Wenn ich auf einer Maschine, die Mitglied einer vertrauten Windows 200x-Domäne ist, ein Windows 200x-Mitglied einer vertrauenden Samba-Domäne durchsuche, bekomme ich folgenden Fehler:

. *Das System hat einen möglichen Angriff auf die Sicherheit festgestellt. Bitte versichern Sie sich, dass Sie Kontakt zu dem Server haben, der Sie authentifiziert.*

Die Event-Logs auf der Maschine, die ich versuche zu erreichen, haben Einträge, die nicht angewendete Gruppen-Richtlinien betreffen, weil diese Maschine ein Mitglied einer untergeordneten Domäne ist.

Antwort: Dieses Problem kann auftreten, wenn ein Computer-Konto für die betroffene Maschine in der Windows 200x-Domäne existiert und diese deaktiviert ist. Falls dieses Computer-Konto nicht existiert (d.h. entfernt oder nie erstellt wurde) oder dieses Konto noch immer intakt ist (z.B.: Sie haben es gerade in eine andere Domäne verschoben), sollte alles in Ordnung sein. Wenn man die Domäne (die Windows 200x-Domäne) verlässt, versucht der Computer normalerweise, automatisch das Computer-Konto zu deaktivieren. Falls während dieses Vorgangs ein Konto verwendet wird, das die Privilegien dazu hat, wird das Computer-Konto deaktiviert, sonst nicht.

15.6.2 Probleme mit LDAP ldapsam und den smbldap-Tools

Wenn Sie das **smbldap-useradd.pl**-Skript benutzen, um ein Konto für die Fertigstellung einer Interdomain-Vertrauensstellung zu erstellen, wird dieser Prozess fehlschlagen. Das Konto, das in der LDAP-Datenbank erstellt wurde, wird ein Konto-Flag-Feld haben, das `[W ]` enthält, wärend es `[I ]` für eine funktionierende Interdomain-Vertrauensstellung enthalten müsste.

*Antwort:*Hier eine einfache Lösung. Erstellen Sie ein Maschinen-Konto wie folgt:

```
root#  smbldap-useradd.pl -w domain_name
```

Dann setzen Sie das Passwort für das gewünschte Vertrauensstellungskonto wie hier:

```
root#  smbldap-passwd.pl domain_name\$
```

Mit einem Texteditor erstellen Sie folgende Datei:

```
dn: uid=domain_name$,ou=People,dc={your-domain},dc={your-top-level-domain}
changetype: modify
sambaAcctFlags: [I          ]
```

Dann fügen Sie die Text-Datei wie folgt zur LDAP-Datenbank hinzu:

```
root#  ldapmodify -x -h localhost \
 -D "cn=Manager,dc={your-domain},dc={your-top-level-domain}" \
 -W -f /path-to/foobar
```

Erstellen Sie eine einseitige Vertrauensstellung mit dem NT4-Domain User Manager, und führen Sie dann Folgedes aus:

```
root#  net rpc trustdom establish domain_name
```

Dies funktioniert mit Samba-3- und NT4-Domänen sowie mit Samba-3 und Windows 200x ADS in gemischtem Modus. Beide DCs, Samba und NT, müssen den gleichen WINS-Server benutzen, sonst wird die Vertrauensstellung nie funktionieren.

Kapitel 16

BETREIBEN EINES MICROSOFT DISTRIBUTED-FILE-SYSTEM-BAUMS

16.1 Eigenschaften und Vorzüge

Das Distributed File System (DFS) erlaubt es, die logische Ansicht der Laufwerke und Ordner, die der Benutzer sieht, von der tatsächlichen physischen Lage dieser Ressourcen im Netzwerk zu trennen. Die Vorteile sind höhere Erreichbarkeit, einfachere Speicherplatzerweiterung, Lastausgleich usw.

Informationen zu DFS finden Sie in der Microsoft Dokumentation <`http://www.microsoft.com/NTServer/nts/downloads/winfeatures/NTSDistrFile/AdminGuide.asp`>. Dieses Dokument erklärt, wie man einen DFS-Baum auf einer UNIX-Maschine (zum Browsing für DFS-fähige Clients) mit Samba betreibt.

Um SMB-basierendes DFS für Samba zu aktivieren, konfigurieren Sie es mit der Option `--with-msdfs`. Wenn das geschehen ist, kann ein Samba-Server zu einem DFS-Server gemacht werden, indem Sie den globalen booleschen Parameter host msdfs in der Datei `smb.conf` setzen. Sie kennzeichnen eine Freigabe als DFS-Wurzelverzeichnis durch den booleschen Freigaben-Parameter msdfs root. Ein DFS-Wurzelverzeichnis unter Samba beinhaltet DFS-Links in der Form von symbolischen Links, die auf andere Server zeigen. So arbeitet zum Beispiel ein symbolischer Link `junction->msdfs:storage1\share1` im Freigabenverzeichnis als die DFS-Junction. Wenn DFS-fähige Clients versuchen, auf diesen Junction-Link zuzugreifen, werden sie auf die tatsächliche Daten-Freigabe weitergeleitet (in diesem Fall ist das *storage1**share1*).

DFS-Bäume unter Samba funktionieren mit allen DFS-fähigen Clients von Windows 95 bis 200x. Beispiel **??** zeigt, wie man einen DFS-Baum auf einem Samba-Server einrichtet. Im Verzeichnis `/export/dfsroot` richten Sie die DFS-Links auf andere Server im Netzwerk ein.

```
root# cd /export/dfsroot
root# chown root /export/dfsroot
root# chmod 755 /export/dfsroot
```

```
root# ln -s msdfs:speicherA\\freigabeA linka
root# ln -s msdfs:serverB\\freigabe,serverC\\freigabe linkb
```

Beispiel 16.1.1. smb.conf mit konfiguriertem DFS

```
[global]
        netbios name = GANDALF
        host msdfs = yes

[dfs]
        path = /export/dfsroot
        msdfs root = yes
```

Sie sollten die Berechtigungen und den Eigentümer des DFS-Wurzelverzeichnisses so setzen, dass nur bestimmte Benutzer die msdfs-Links anlegen, löschen oder verändern können. Beachten Sie auch, dass die Symlink-Namen alle in Kleinschreibung angegeben werden. Diese Einschränkung existiert, um zu vermeiden, dass Samba alle Schreibweisen durchprobiert, um zu dem Linknamen zu gelangen. Zum Abschluss richten Sie die symbolischen Links so ein, dass sie auf die gewünschten Netzwerkfreigaben zeigen, und starten Samba.

Jetzt können Benutzer auf den DFS-fähigen Clients unter \\samba\dfs den DFS-Baum durchsuchen. Zugriffe auf die Links linka oder linkb (die dem Client als Verzeichnisse erscheinen) führen die Benutzer direkt auf die entsprechenden Netzwerk-Freigaben.

16.2 Gängige Fehler

- Windows-Clients müssen rebootet werden, wenn eine zuvor gemountete Nicht-DFS-Freigabe zu einem DFS-Wurzelverzeichnis gemacht wird, oder umgekehrt. Eine bessere Lösung ist, eine neue Freigabe zum DFS-Wurzelverzeichnis zu machen.
- Derzeit herrscht die Einschränkung, dass alle msdfs-Symlinks in Kleinschreibung benannt werden müssen.
- Aus Sicherheitsgründen sollte das DFS-Wurzelverzeichnis Eigentümer und Berechtigungen so gesetzt haben, dass nur bestimmte Benutzer die Symlinks in diesem Verzeichnis verändern können.

16.2.1 Der MSDFS-UNIX-Pfad ist „*case-critical*“

Ein Netzwerk-Administrator sandte folgenden Rat an die Samba-Mailing-Liste, nachdem er in langen Sitzungen versucht hatte herauszufinden, warum DFS nicht funktionierte. Sein Rat ist beachtenswert.

„*Ich habe einige Zeit damit verbracht herauszufinden, warum mein dfs root nicht funktioniert. In der Dokumentation steht, dass der Symlink in Kleinschreibung benannt werden muss. Dies sollte dahingehend berichtigt werden, dass der gesamte Pfad zu dem Symlink auch in Kleinschreibung angegeben werden muss.*“

Zum Beispiel hatte ich eine Freigabe so definiert:

```
[pub]
   path = /export/home/Shares/public_share
   msdfs root = yes
```

und konnte mein Windows 9x/Me (mit installiertem DFS-Client) nicht dazu bringen, diesem Symlink zu folgen:

```
damage1 -> msdfs:damage\test-share
```

Der Debug-Level 10 enthüllte:

```
[2003/08/20 11:40:33, 5] msdfs/msdfs.c:is_msdfs_link(176)
  is_msdfs_link: /export/home/shares/public_share/* does not exist.
```

Ich wurde neugierig. Also änderte ich den Verzeichnisnamen von .../Shares/... in .../shares/... (wie auch meine Freigaben-Definition), und es funktionierte!

Kapitel 17

KLASSISCHE DRUCKERUNTERSTÜTZUNG

17.1 Eigenschaften und Vorzüge

Die Möglichkeit, etwas drucken zu können, ist für viele Benutzer oft eine Dienstleistung von zentraler Bedeutung. Samba kann diese in einem Netz von Windows-Clients zuverlässig und nahtlos zur Verfügung stellen.

Ein Samba-Druckdienst kann auf einem Stand-alone- oder Domänenmitgliedsserver betrieben werden, gemeinsam mit Dateiserver-Funktionen, oder auch auf einem eigenen Druckserver. Seine Sicherheit kann je nach Bedarf zwischen sehr hoch und sehr niedrig gewählt werden. Die Konfiguration kann einfach oder komplex sein. Die verfügbaren Authentifizierungsschemata sind im Wesentlichen die gleichen, die in den vorigen Kapiteln auch bei Dateidiensten beschrieben wurden. Alles in allem kann die Druckerunterstützung von Samba einen NT- oder Windows 2000-Druckerserver vollständig ersetzen, oft mit zusätzlichen Vorteilen. Clients können mit Hilfe des bekannten „*Point'n'Print*"-Mechanismus Treiber herunterladen und sie auf Druckern installieren. Die Installation von Druckern über „*Anmeldeskripten*" ist kein Problem. Administratoren können Treiber, die von Clients benutzt werden sollen, mit dem bekannten „*Assistenten für die Druckerinstallation*" (engl. „*Add Printer Wizard*", APW) hochladen und verwalten. Ein weiterer Vorteil ist der, dass die Treiber- und Druckerverwaltung über die Kommandozeile oder mit Hilfe von Skripten ausgeführt werden kann, was bei einer großen Anzahl von Druckern effizienter ist. Falls eine zentrale Buchführung(((Verwaltung?))) der Druckaufträge benötigt wird (Beobachtung jeder einzelnen Seite und Weitergabe der Rohdaten für alle möglichen statistischen Berichte), so wird diese Funktion am besten durch das neue Common UNIX Printing System (CUPS), das Drucksubsystem unter der Samba-Oberfläche, unterstützt.

Dieses Kapitel behandelt die Grundlagen des Druckens mit Samba, wie sie von den traditionelleren Drucksystemen in UNIX (BSD- und System V-ähnliche) implementiert sind. Vieles, was in diesem Kapitel abgedeckt wird, gilt auch für CUPS. Falls Sie CUPS benutzen, sind Sie vielleicht versucht, zum nächsten Kapitel zu springen, aber in dem Fall würden Sie bestimmt einiges verpassen. Es wird empfohlen, dass Sie dieses Kapitel ebenso wie das Kapitel Unterstützung des CUPS-Drucksystems lesen.

Anmerkung

Die meisten der folgenden Beispiele wurden auf Rechnern mit Windows XP Professional überprüft. Dort, wo dieses Dokument die Antworten zu eingegebenen Befehlen beschreibt, sollten Sie bedenken, dass Windows 200x/XP-Rechner zwar sehr ähnlich sind, sich aber in geringfügigen Details unterscheiden können. Windows NT ist zusätzlich noch ein wenig anders.

17.2 Technische Informationen

Sambas Druckerunterstützung basiert immer auf dem installierten Drucksubsystem des UNIX-Betriebssystems, auf dem es läuft. Samba nimmt damit die Rolle eines „*Vermittlers*“ ein. Es nimmt Druckdateien von Windows- (oder anderen SMB-)Clients an und gibt sie an das eigentliche Drucksystem weiter, das sie bearbeitet, d.h., es muss mit beiden Seiten kommunizieren: sowohl mit den Drucker-Clients unter Windows als auch mit dem Drucksystem von UNIX. Daher müssen wir zwischen verschiedenen Arten von Betriebssystem-Clients unterscheiden, die sich alle unterschiedlich verhalten, ebenso wie zwischen den verschiedenen Drucksystemen von UNIX, die ihrerseits verschiedene Eigenschaften haben und unterschiedlich angesprochen werden.

An dieser Stelle wird die traditionelle Art des Druckens unter UNIX behandelt. Das nächste Kapitel behandelt detailliert das modernere *Common UNIX Printing System* (CUPS).

Wichtig

CUPS-Benutzer, seien Sie gewarnt: Springen Sie nicht einfach zum nächsten Kapitel weiter, sonst verpassen Sie eventuell wichtige Informationen, die Sie nur hier finden!

Aus den Beiträgen auf der Samba-Mailingliste geht hervor, dass die Druckerkonfiguration heute einer der problematischsten Aspekte bei der Administration von Samba ist. Viele neue Samba-Administratoren gewinnen den Eindruck, dass Samba irgendeinen Teil des Druckvorgangs selbst übernimmt. Seien Sie jedoch versichert, dass Samba keinerlei Verarbeitung beim Drucken selbst durchführt. Es agiert in keiner Weise als Druckerfilter.

Von seinen Clients bekommt Samba einen Datenstrom (den Druckauftrag), den es an ein lokales Spooling-Verzeichnis leitet. Nachdem der gesamte Druckauftrag empfangen wurde, führt Samba einen lokalen UNIX/Linux-Druckbefehl aus und übergibt ihm die erhaltene Datei. Es ist die Aufgabe der Drucksubsysteme des lokalen Systems, den Druckauftrag korrekt zu bearbeiten und ihn an den Drucker zu übergeben.

17.2.1 Übergabe eines Druckauftrags vom Client an Samba

Um von einem Windows-Client einen Druckauftrag über einen Samba-Druckserver an einen UNIX-Drucker zu senden, sind sechs (manchmal sieben) Stadien erforderlich:

1. Windows öffnet eine Verbindung zur Druckerfreigabe.
2. Samba muss den Benutzer authentifizieren.
3. Windows sendet eine Kopie der Druckdatei über das Netzwerk in den Spooling-Bereich von Samba.
4. Windows trennt die Verbindung.
5. Samba führt den Druckbefehl aus, mit dem die Datei in den Spooling-Bereich des UNIX-Drucksubsystems übergeben wird.
6. Das UNIX-Drucksubsystem bearbeitet den Druckauftrag.
7. Die Druckdatei muss eventuell explizit aus dem Spooling-Bereich von Samba gelöscht werden. Dieser Punkt hängt von den Konfigurationseinstellungen Ihres Druck-Spoolers ab.

17.2.2 Druckrelevante Konfigurationsparameter

Es gibt eine Reihe von Konfigurationsparametern, mit denen man Sambas Druckverhalten steuern kann. Bitte sehen Sie sich die Manpage zu `smb.conf` an, um eine Übersicht darüber zu erhalten. Wie bei anderen Parametern gibt es auch hier Parameter auf einer globalen Ebene (in den Listings mit einem *G* markiert) und solche auf einer Serviceebene (*S*).

Globale Parameter Diese *dürfen nicht* in die individuellen Freigabedefinitionen eingehen. Wenn sie dort irrtümlich eingehen, kann das Utility **testparm** das feststellen und es Ihnen mitteilen (sofern Sie es starten).

Serviceebenen-Parameter Diese dürfen im Abschnitt *[global]* von `smb.conf` angegeben werden. In diesem Fall definieren sie das Standardverhalten von allen individuellen Freigaben oder von Freigaben auf Serviceebene (vorausgesetzt, es gibt keine andere Einstellung für den gleichen Parameter, der die globale Voreinstellung überschreibt).

17.3 Einfache Druckkonfiguration

Das folgende Beispiel zeigt eine einfache Druckkonfiguration. Wenn Sie diese mit Ihrer eigenen vergleichen, finden Sie eventuell zusätzliche Parameter, die vom Verkäufer Ihres Betriebssystems vorkonfiguriert wurden. Darunter befindet sich eine Beschreibung und Erläuterung dieser Parameter. In diesem Beispiel werden nur wenige Parameter verwendet. In vielen Umgebungen reichen sie jedoch aus, um damit eine gültige Datei `smb.conf` zur Verfügung zu stellen, mit der alle Clients drucken können.

Dies ist lediglich eine Beispielkonfiguration. Samba weist allen Konfigurationsparametern Standardwerte zu. Diese Werte sind empfindlich und wurden mit mit Bedacht gewählt.

Beispiel 17.3.1. Einfache Konfiguration mit BSD-Drucken

```
[global]
       printing = bsd
       load printers = yes

[printers]
       path = /var/spool/samba
       printable = yes
       public = yes
       writable = no
```

Wenn ein Parameter in der Datei `smb.conf` angegeben ist, dann überschreibt er den Standardwert. Das Utility namens **testparm** kann alle Einstellungen ausgeben, wenn es unter root ausgeführt wird - Standardwerte ebenso wie Einträge in der Datei `smb.conf`. Für alle fehlerhaft konfigurierten Einstellungen gibt **testparm** eine Warnung aus. Die vollständige Ausgabe erreicht leicht 340 Zeilen und mehr, d.h., Sie werden sie vermutlich mit einem Programm zum Durchblättern anschauen wollen.

Die Syntax der Konfigurationsdatei ist leicht zu verstehen. Sie sollten wissen, dass Samba es mit seiner Syntax nicht sehr genau nimmt. Wie schon an anderer Stelle in diesem Dokument erklärt wurde, toleriert Samba einige Schreibfehler (z.B. browseable an Stelle von browseable), wobei die Schreibweise (groß/klein) irrelevant ist. Es ist zulässig, für boolesche Einstellungen *Yes/No* oder *True/False* zu verwenden. Listen von Namen dürfen mit Kommas, Leerzeichen oder Tabulatoren getrennt werden.

17.3.1 Überprüfen der Konfiguration mit testparm

Um alle (oder wenigstens die meisten) druckerrelevanten Einstellungen in Samba zu sehen, inklusive derer, die implizit verwendet werden, können Sie den unten angegebenen Befehl ausprobieren. Dieser sucht nach allen Vorkommen von `lp, print, spool, driver, ports` und `[` in der Ausgabe von testparms, was eine bequeme Übersicht über die aktuelle Druckerkonfiguration von **smbd** ergibt. Dieser Befehl zeigt keine individuell erstellten Druckerfreigaben oder die Spooling-Pfade an, die sie eventuell benutzen. Folgendes ist die Ausgabe meiner Samba-Einstellung, mit den Einstellungen, die im vorherigen Beispiel gezeigt wurden:

```
root# testparm -s -v | egrep "(lp|print|spool|driver|ports|\[)"
 Load smb config files from /etc/samba/smb.conf
 Processing section "[homes]"
 Processing section "[printers]"

 [global]
        smb ports = 445 139
        lpq cache time = 10
        total print jobs = 0
```

```
        load printers = Yes
        printcap name = /etc/printcap
        disable spoolss = No
        enumports command =
        addprinter command =
        deleteprinter command =
        show add printer wizard = Yes
        os2 driver map =
        printer admin =
        min print space = 0
        max print jobs = 1000
        printable = No
        printing = bsd
        print command = lpr -r -P'%p' %s
        lpq command = lpq -P'%p'
        lprm command = lprm -P'%p' %j
        lppause command =
        lpresume command =
        printer name =
        use client driver = No

[homes]

[printers]
        path = /var/spool/samba
        printable = Yes
```

Sie können ganz leicht überprüfen, welche Einstellungen dank Sambas Standardverhalten implizit hinzugefügt werden. *Nicht vergessen: Das könnte für Ihren späteren Umgang mit Samba von Bedeutung sein.*

ANMERKUNG

testparm in Samba-3 verhält sich anders als testparm in Samba 2.2.x: Ohne den Schalter „*-v*“ zeigt es Ihnen nur die Einstellungen, in die geschrieben wird! Um die vollständige benutzte Konfiguration zu sehen, verwenden Sie bei testparm den Schalter „*-v*“.

17.3.2 Schnelle Validierung der Konfiguration

Sollten Sie in irgendeinem Stadium Reparaturen vornehmen müssen, kommen Sie bitte immer erst an diesen Punkt zurück, und überprüfen Sie, ob **testparm** die Parameter anzeigt, die Sie erwarten. Aus eigener Erfahrung erhalten Sie hier den Hinweis, es einmal mit dem

Auskommentieren des Parameters load printers zu versuchen. Falls Ihr System 2.2.x sich so verhält wie meines, werden Sie Folgendes sehen:

```
root# grep "load printers" /etc/samba/smb.conf
        #  load printers = Yes
        # Diese Einstellung ist auskommentiert!!

root# testparm -v /etc/samba/smb.conf | egrep "(load printers)"
        load printers = Yes
```

Ich nahm an, dass durch das Auskommentieren dieser Einstellung Samba meine Drucker nicht mehr anzeigen würde, was es aber weiterhin tat. Ich habe eine Weile gebraucht, um den Grund dafür herauszufinden. Aber nun lasse ich mich nicht mehr foppen... jedenfalls nicht hiervon.

```
root# grep -A1 "load printers" /etc/samba/smb.conf
        load printers = No
        # Obige Einstellung ist, was ich will!
        #  load printers = Yes
        # Diese Einstellung ist auskommentiert!

root# testparm -s -v smb.conf.simpleprinting | egrep "(load printers)"
        load printers = No
```

Nur dann, wenn der Parameter explizit auf load printers = No gesetzt ist, wird Samba das tun, was ich möchte. Daher empfehle ich wärmstens:

- Verlassen Sie sich nie auf auskommentierte Parameter!
- Setzen Sie Parameter immer explizit so, wie Sie wollen, dass sie sich verhalten sollen!
- Verwenden Sie **testparm**, um versteckte Einstellungen aufzudecken, die nicht mit Ihren Absichten übereinstimmen!

Folgendes ist die minimal kleinste Konfigurationsdatei:

```
root# cat /etc/samba/smb.conf-minimal
        [printers]
```

Dieses Beispiel soll Ihnen zeigen, dass Sie testparm benutzen können, um alle Konfigurationsdateien von Samba zu testen. Tatsächlich möchten wir Sie dazu anhalten, Ihr laufendes System *nicht* zu verändern (es sei denn, Sie wissen genau, was Sie tun). Verlassen Sie sich nicht darauf, dass die Änderungen erst dann wirksam werden, nachdem Sie smbd neu starten! Das ist nicht der Fall. Samba liest sie alle 60 Sekunden erneut ein, und zwar auf jeder neuen Client-Verbindung. Möglicherweise werden Sie mit Änderungen auf Ihren Clients in Produktion konfrontiert, die Sie gar nicht vornehmen wollten. Sie werden nun einige weitere

interessante Dinge bemerken: **testparm** hilft Ihnen dabei festzustellen, was die Samba-Druckerkonfiguration wäre, wenn Sie diese minimale Konfiguration benutzen würden. Folgendes können Sie dabei erwarten:

```
root# testparm -v smb.conf-minimal | egrep "(print|lpq|spool|driver|ports|[)"
 Processing section "[printers]"
 WARNING: [printers] service MUST be printable!
 No path in service printers - using /tmp

        lpq cache time = 10
        total print jobs = 0
        load printers = Yes
        printcap name = /etc/printcap
        disable spoolss = No
        enumports command =
        addprinter command =
        deleteprinter command =
        show add printer wizard = Yes
        os2 driver map =
        printer admin =
        min print space = 0
        max print jobs = 1000
        printable = No
        printing = bsd
        print command = lpr -r -P%p %s
        lpq command = lpq -P%p
        printer name =
        use client driver = No

 [printers]
        printable = Yes
```

testparm hat zwei Warnungen ausgegeben:

- Wir haben nicht angegeben, dass der Abschnitt *[printers]* druckbar ist.
- Wir haben Samba nicht gesagt, welches Spooling-Verzeichnis verwendet werden soll.

Beides ist allerdings nicht so schlimm, und Samba greift daher auf funktionierende Standardwerte zurück. Bitte verlassen Sie sich jedoch nicht darauf, und verwenden Sie dieses Beispiel nicht selbst. Es ist hier nur deswegen erwähnt, um Ihnen zu sagen, dass Sie Ihre Einstellungen vorsichtig entwerfen und vornehmen sollen, damit genau das passiert, was Sie haben möchten. Auf Ihrem System mag das Resultat bei einigen der angegebenen Parameter leicht abweichen, da Samba möglicherweise mit anderen Optionen kompiliert wurde. *Warnung:* Setzen Sie kein Kommentarzeichen *ans Ende* einer gültigen Zeile. Das bewirkt, dass der Parameter ignoriert wird (so, als ob Sie das Kommentarzeichen an den Zeilenanfang gesetzt hätten). Zu Beginn hielt ich das für einen Fehler in meinen Samba-Versionen. Aber

die Manpage sagt es deutlich: „*Interner Leerraum in einem Parameterwert wird wörtlich erhalten.*“ Das bedeutet, dass z.B. eine Zeile, die aus

```
# Dies definiert LPRng als das Drucksystem
        printing = lprng
```

besteht, den gesamten String nach dem Zeichen „=“ als den gewünschten Wert betrachtet, den Sie definieren möchten. Dies ist jedoch ein ungültiger Wert, der ignoriert und durch einen Standardwert ersetzt wird.

17.4 Erweiterte Druckerkonfiguration

Die nächste Konfiguration zeigt ein etwas umfangreicheres Beispiel einer Konfiguration von druckrelevanten Einstellungen in einer BSD-artigen Druckumgebung. Anschließend werden die verschiedenen Parameter beschrieben und erklärt. Wir haben hier deswegen BSD-artiges Drucken ausgewählt, weil es immer noch das am meisten verwendete System auf schon vorhandenen UNIX/Linux-Installationen ist. Neue Installationen verwenden überwiegend CUPS, das in einem eigenen Kapitel beschrieben wird. Das Beispiel führt die Namen vieler Parameter explizit auf, die nicht angegeben werden müssen, da sie standardmäßig gesetzt werden. Sie könnten auch eine wesentlich leichtere `smb.conf`-Datei verwenden. Alternativ dazu können Sie **testparm** oder **SWAT** benutzen, um die Datei `smb.conf` zu optimieren und alle Parameter zu entfernen, die standardmäßig gesetzt werden.

Dies ist eine Beispielkonfiguration. Möglicherweise finden Sie nicht alle Einstellungen in der Konfigurationsdatei, die vom Betriebssystemhersteller mitgeliefert wurde. Samba verwendet für Konfigurationsparameter, die nicht explizit gesetzt sind, einen sinnvollen Standardwert. Sie können sich alle Einstellungen anschauen, indem Sie als `root` das Utility **testparm** benutzen. Mit Hilfe von **testparm** erhalten Sie Warnungen bei fehlerhaft konfigurierten Einstellungen.

17.4.1 Detaillierte Erörterung der Einstellungen

Die folgende Erörterung beschreibt die Einstellungen des obigen Beispiels.

17.4.1.1 Der Abschnitt [global]

Der Abschnitt *[global]* ist einer von vier besonderen Abschnitten (zusammen mit *[homes]*, *[printers]* und *[print$]*...). Unter *[global]* sind alle Parameter enthalten, die für den Server als Ganzes gelten. Hier stehen Parameter, die nur global eine Bedeutung haben. Es dürfen auch Parameter auf Serviceebene enthalten sein, die dann Standardeinstellungen für alle anderen Abschnitte und Freigaben definieren. Auf diese Weise können Sie die Konfiguration vereinfachen und vermeiden, den gleichen Wert mehrfach zu setzen. (Innerhalb jedes einzelnen Abschnitts bzw. jeder Freigabe dürfen Sie diese global gesetzten Freigabeeinstellungen allerdings überschreiben und andere Werte dafür angeben).

printing = bsd Bewirkt, dass Samba die Standarddruckbefehle verwendet, die im BSD-Drucksystem (auch als RFC 1179 oder LPR/LPD bekannt) vorgesehen sind. Im

Beispiel 17.4.1. Erweiterte BSD-Druckerkonfiguration

```
[global]
       printing = bsd
       load printers = yes
       show add printer wizard = yes
       printcap name = /etc/printcap
       printer admin = @ntadmin, root
       total print jobs = 100
       lpq cache time = 20
       use client driver = no

[printers]
       comment = Alle Drucker
       printable = yes
       path = /var/spool/samba
       browseable = no
       guest ok = yes
       public = yes
       read only = yes
       writable = no

[my_printer_name]
       comment = Drucker mit beschraenktem Zugriff
       path = /var/spool/samba_my_printer
       printer admin = kurt
       browseable = yes
       printable = yes
       writable = no
       hosts allow = 0.0.0.0
       hosts deny = turbo_xp, 10.160.50.23, 10.160.51.60
       guest ok = no
```

Allgemeinen informiert der Parameter *printing* Samba über das Drucksubsystem, mit dem es rechnen soll. Samba unterstützt CUPS, LPD, LPRNG, SYSV, HPUX, AIX, QNX und PLP. Jedes dieser Systeme hat seinen eigenen Druckbefehl (sowie andere Befehle zur Steuerung der Druckerschlange).

> ACHTUNG
>
> Der Parameter printing ist normalerweise ein Parameter der Service-Ebene. Da er hier im Abschnitt *[global]* enthalten ist, wird er für alle Druckerfreigaben wirksam, für die nichts anderes definiert ist. Samba-3 unterstützt das Drucksystem SOFTQ nicht mehr.

load printers = yes Weist Samba an, automatisch alle verfügbaren Druckerfreigaben zu erstellen. Verfügbare Druckerfreigaben werden beim Scannen der Datei printcap entdeckt. Alle erstellten Druckerfreigaben werden auch zum Browsen geladen. Falls Sie diesen Parameter verwenden, müssen Sie keine separaten Freigaben für jeden Drucker angeben. Jede automatisch erstellte Druckerfreigabe erstellt einen Klon von den Konfigurationsoptionen im Abschnitt *[printers]*. (Die Einstellung *load printers = no* erlaubt Ihnen, jeden gemeinsam genutzten UNIX-Drucker separat anzugeben, wobei Sie einige auslassen können, bei denen Sie nicht möchten, dass sie öffentlich sichtbar und verfügbar sind).

show add printer wizard = yes Diese Einstellung ist normalerweise standardmäßig aktiviert (sogar dann, wenn der Parameter nicht in `smb.conf` angegeben ist). Sie bewirkt, dass das Icon **Assistent für die Druckerinstallation** im Verzeichnis **Drucker** der Freigabeliste des Samba-Hosts erscheint (wie es in **Netzwerkumgebung** oder vom Befehl **net view** gezeigt wird). Um diese Einstellung zu deaktivieren, müssen Sie sie explizit auf `no` setzen (nur auskommentieren reicht nicht). Mit dem *Assistenten für die Druckerinstallation* können Sie Druckertreiber auf die Freigabe *[print$]* hochladen und sie mit einem Drucker verbinden (falls die entsprechende Schlange vorher schon existiert) oder den Treiber eines Drucker gegen einen anderen vorher hochgeladenen Treiber austauschen.

total print jobs = 100 Setzt die obere Grenze der gleichzeitig auf dem Samba-Server aktiven Druckaufträge auf 100. Sollte ein Client einen Auftrag mit einer höheren Nummer absetzen, erhält er von Samba eine Fehlermeldung der Art „*no more space available on server*“. Der Wert Null (die Voreinstellung) bedeutet, dass es *keine* Beschränkung gibt.

printcap name = /etc/printcap Sagt Samba, wo es nach einer Liste verfügbarer Druckernamen suchen soll. Wenn CUPS verwendet wird, sollten Sie sicherstellen, dass eine printcap-Datei geschrieben wird, was mit der Direktive `Printcap` in der Datei `cupsd.conf` gesteuert wird.

printer admin = @ntadmin Mitglieder der Gruppe ntadmin sollten in der Lage sein, Treiber hizuzufügen und Druckereigenschaften zu setzen (`ntadmin` ist lediglich ein Beispielname, es muss der Name einer gültigen UNIX-Gruppe sein); root ist implizit immer ein printer admin. Das Zeichen @ steht vor Gruppennamen in `/etc/group`. Ein

printer admin kann mit den MS-RPC-Schnittstellen für die Fernwartung (siehe unten) alles Mögliche mit Druckern anstellen. In größeren Installationen gibt es normalerweise je einen Parameter printer admin pro Freigabe. Damit können alle Druckerfreigaben von verschiedenen Gruppen verwaltet werden.

lpq cache time = 20 Gibt die Cache-Zeit für die Ergebnisse des Befehls lpq an. Sie verhindert, dass der lpq-Befehl zu oft aufgerufen wird, und reduziert so die Last auf einem stark ausgelastetem Druckserver.

use client driver = no Falls er auf `yes` gesetzt ist, wirkt sich dieser Parameter nur auf Windows NT/200x/XP-Clients aus (und nicht auf Win 95/98/ME). Sein Standardwert ist `No` (oder `False`). Er darf bei Druckerfreigaben, für die auf dem Samba-Server gültige Treiber installiert sind, *nicht* aktiviert werden (mit der Einstellung `yes` oder `true`). Eine detailliertere Erklärung finden Sie in der Manpage zu `smb.conf`.

17.4.1.2 Der Abschnitt [printers]

Dies ist der zweite besondere Abschnitt. Falls ein Abschnitt mit diesem Namen in `smb.conf` vorkommt, können die Benutzer sich mit jedem Drucker verbinden, der in der printcap-Datei des Samba-Hosts angegeben ist, da Samba dann beim Hochfahren eine Druckerfreigabe für jeden Druckernamen erstellt, den es in der Datei printcap findet. Das könnte man als allgemeine bequeme Abkürzung dafür sehen, alle Drucker mit minimaler Konfiguration freizugeben. Dieser Abschnitt ist auch ein Container für Einstellungen, die für alle Drucker gelten sollen. (Weitere Details finden Sie auf der Manpage zu `smb.conf`.) Die Einstellungen in diesem Container müssen Parameter auf der Ebene der Freigabe sein.

comment = Alle Drucker Der Kommentar wird neben der Freigabe angezeigt, wenn ein Client beim Server anfragt, und zwar entweder mit **Netzwerkumgebung** oder mit dem Befehl **net view**, der verfügbare Freigaben auflistet.

printable = yes Der Dienst *`[printers]` muss* muss als printable, d.h. druckbar deklariert werden. Anderenfalls weigert sich smbd, beim Hochfahren etwas zu laden. Dieser Parameter ermöglicht es verbundenen Clients, Sppol-Dateien zu öffnen, darin zu schreiben und sie in das Verzeichnis zu übertragen, das mit dem Parameter path für diesen Dienst angegeben wird. Samba verwendet ihn, um Druckerfreigaben von Dateifreigaben zu unterscheiden.

path = /var/spool/samba Das muss der Name eines Verzeichnisses sein, das Samba beim Spoolen ankommender Druckdateien verwendet. *Es darf nicht identisch sein mit mit dem Spooling-Verzeichnis, das in der Konfiguration Ihres UNIX-Drucksubsystems angegeben ist!* Der Pfad beschreibt normalerweise ein Verzeichnis, in dem alle Schreibrechte haben und dessen „*sticky*“-Bit gesetzt ist.

browseable = no Ist immer auf `no` gesetzt, falls printable = yes. Dadurch wird die Freigabe *`[printer]`* selbst in der Liste der verfügbaren Freigaben bei dem Befehl

net view oder in der Browserliste des Explorers unsichtbar. (Natürlich können Sie die einzelnen Drucker noch sehen).

guest ok = yes Falls dieser Parameter auf `yes` gesetzt ist, wird kein Passwort für eine Verbindung zu diesem Druckdienst benötigt. Der Zugang erfolgt mit den Rechten des Gast-Kontos. Auf vielen Systemen wird das Gast-Konto auf einen Benutzer namens „*nobody*“ abgebildet. Für diesen Benutzer findet UNIX normalerweise in der Datei passwd ein leeres Passwort vor, aber kein gültiges UNIX-Login. (Auf manchen Systemen hat das Gast-Konto eventuell keine Druckrechte. Testen Sie das, indem Sie sich mit **su - guest** als Gastbenutzer anmelden, und geben Sie wie folgt einen Druckbefehl im System ein:

```
lpr -P printername /etc/motd
```

public = yes Ist ein Synonym für guest ok = yes. Da wir guest ok = yes haben, muss das hier nicht wirklich stehen. (Das führt zu der interessanten Frage: „*Was passiert, falls wir irrtümlicherweise zwei widersprüchliche Einstellungen für die gleiche Freigabe haben?*“ Die Antwort lautet, dass die letzte von Samba gefundene Einstellung gewinnt. Testparm beschwert sich nicht über verschiedene Einstellungen beim gleichen Parameter für eine Freigabe. Das können Sie testen, indem Sie mehrere Zeilen für den Parameter *`guest account`* mit verschiedenen Benutzernamen eintragen und dann testparm ausführen, um zu sehen, welchen Samba tatsächlich benutzt.)

read only = yes Verhindert normalerweise, d.h. bei anderen Arten von Freigaben, dass Benutzer Dateien im Dienstverzeichnis erstellen oder modifizieren. Bei dem Dienst „*printable*“ ist es allerdings *immer* erlaubt, ins Verzeichnis zu schreiben (falls die Rechte des Benutzers eine Verbindung erlauben), jedoch nur mit Hilfe von Drucker-Spooling-Operationen. Normale Schreiboperationen sind nicht erlaubt.

writable = no Ist ein Synonym für read only = yes.

17.4.1.3 Beliebige Abschnitte [mein_drucker_name]

Wenn ein Abschnitt in der Datei `smb.conf` vorkommt und den Parameter printable = yes enthält, dann konfiguriert ihn Samba als Druckerfreigabe. Windows 9x/Me-Clients haben eventuell Probleme damit, sich mit Druckertreibern zu verbinden oder sie zu laden, wenn der Name der Freigabe mehr als acht Zeichen lang ist. Geben Sie einer Druckerfreigabe keinen Namen, der mit einer vorhandenen Benutzer- oder Dateifreigabe kollidieren könnte. Bei Verbindungsanfragen von Clients versucht Samba immer zuerst Dateifreigaben mit diesem Namen zu finden. Wenn Samba eine findet, stellt es damit eine Verbindung her und nicht mit dem gleichnamigen Drucker!

comment = Drucker mit beschraenktem Zugriff Der Kommentar sagt alles aus.

path = /var/spool/samba_my_printer Setzt den Spooling-Bereich für diesen Drucker auf ein Verzeichnis, das sich vom Standardwert unterscheidet. Man muss ihn nicht anders setzen, aber die Möglichkeit ist vorhanden.

printer admin = kurt Die Definition von printer admin unterscheidet sich für diese explizit definierte Druckerfreigabe von der allgemeinen Freigabe *[printers]*. Dies ist nicht notwendig, wir machen das nur, um zu zeigen, dass es möglich ist.

browseable = yes Damit kann man den Drucker aufstöbern, d.h. die Clients können ihn bequem finden, wenn sie in der **Netzwerkumgebung** stöbern.

printable = yes Siehe Der(((den?))) Abschnitt [printers].

writable = no Siehe Der(((den?))) Abschnitt [printers].

hosts allow = 10.160.50.,10.160.51. Hier führen wir ein gewisses Maß an Zugangskontrolle aus, indem wir die Parameter hosts allow und hosts deny verwenden. Das ist keinesfalls eine sichere Maßnahme. Es ist keine sichere Methode, Ihre Drucker abzusichern. Mit dieser Zeile werden alle Clients aus einem bestimmten Subnetz in einer ersten Auswertung der Zugangskontrolle akzeptiert.

hosts deny = turbo_xp,10.160.50.23,10.160.51.60 Alle hier aufgeführten Hosts sind nicht erlaubt (auch dann nicht, wenn sie zu den erlaubten Subnetzen gehören). Wie Sie sehen, können Sie hier IP-Adressen ebenso wie NetBIOS-Hostnamen angeben.

guest ok = no Der Drucker ist für das Gast-Konto nicht verfügbar.

17.4.1.4 Druckbefehle

In jedem Abschnitt, der einen Drucker definiert (oder im Abschnitt *[printers]*), darf ein Parameter namens *print command* definiert werden. Er setzt einen Befehl, mit dem die Dateien bearbeitet werden, die für diesen Drucker in Sambas Drucker-Spooling-Verzeichnis platziert wurden. (Wie Sie sich vielleicht erinnern, wurde dieses Spooling-Verzeichnis mit dem Parameter path eingestellt). Üblicherweise übergibt dieser Befehl die Spool-Datei an das Drucksubsystem des Samba-Hosts, wobei der dem System entsprechende Druckbefehl verwendet wird. Aber es gibt keine Notwendigkeit dafür, dass das so sein muss. Bei der Fehlersuche oder auch aus anderen Gründen möchten Sie eventuell etwas ganz anderes tun, als die Datei zu drucken. Ein Beispiel könnte ein Befehl sein, der die Druckdatei einfach nur an einen temporären Ort kopiert, um sie später untersuchen zu können, wenn Sie Fehler beim Drucken suchen. Wenn Sie an eigenen Druckbefehlen arbeiten (oder gar Shell-Skripten für Druckbefehle entwickeln), sollten Sie darauf aufpassen, dass Sie die Dateien aus dem Spool-Verzeichnis von Samba auch wieder entfernen. Sonst leidet Ihre Festplatte vielleicht schon bald unter Problemen mit fehlendem freien Platz.

17.4.1.5 Standard-Systemdruckbefehle unter UNIX

Sie haben bereits gelernt, dass Samba in den meisten Fällen für viele Parameter seine eingebauten Einstellungen verwendet, wenn es in seiner Konfigurationsdatei keine expliziten Werte dafür findet. Das Gleiche gilt bei der Option print command. Der standardmäßige Druckbefehl variiert abhängig von der Einstellung des Parameters printing. In den unten aufgeführten Befehlen werden Sie einige Parameter der Form *%X* bemerken, wobei *X p, s, J* und so weiter sein kann. Diese Buchstaben stehen jeweils für den Druckernamen, die Spool-Datei und die Job-ID. Sie werden weiter unten detaillierter erklärt. Die nächste Tabelle enthält eine Übersicht der wichtigsten Druckoptionen mit Ausnahme des Spezialfalls CUPS, der im Abschnitt Unterstützung des CUPS-Drucksystems diskutiert wird.

Tabelle 17.1. Standardmäßige Druckereinstellungen

Einstellung	Standardmäßige Druckbefehle
printing = bsd|aix|lprng|plp	Druckbefehl ist **lpr -r -P%p %s**
printing = sysv|hpux	Druckbefehl ist **lp -c -P%p %s; rm %s**
printing = qnx	Druckbefehl ist **lp -r -P%p -s %s**
printing = bsd|aix|lprng|plp	lpq-Befehl ist **lpq -P%p**
printing = sysv|hpux	lpq-Befehl ist **lpstat -o%p**
printing = qnx	lpq-Befehl ist **lpq -P%p**
printing = bsd|aix|lprng|plp	lprm-Befehl ist **lprm -P%p %j**
printing = sysv|hpux	lprm-Befehl ist **cancel %p-%j**
printing = qnx	lprm-Befehl ist **cancel %p-%j**
printing = bsd|aix|lprng|plp	lppause-Befehl ist **lp -i %p-%j -H hold**
printing = sysv|hpux	lppause-Befehl (...ist leer)
printing = qnx	lppause-Befehl (...ist leer)
printing = bsd|aix|lprng|plp	lpresume-Befehl ist **lp -i %p-%j -H resume**
printing = sysv|hpux	lpresume-Befehl (...ist leer)
printing = qnx	lpresume-Befehl (...ist leer)

Wir haben hier den Spezialfall CUPS ausgeklammert, weil er im folgenden Kapitel beschrieben wird. Bei *printing = CUPS* und falls Samba mit libcups kompiliert wurde, verwendet es die CUPS-API, um Druckaufträge einzureichen. (Es ist eine gute Idee, auch printcap = cups zu setzen, falls Ihre `cupsd.conf` so eingestellt ist, dass ihre automatisch generierte printcap-Datei an einen ungewöhnlichen Ort geschrieben wird). Sonst schaltet Samba auf die Druckbefehle von System V um und verwendet beim Drucken die Option -oraw, d.h., es führt den Befehl **lp -c -d%p -oraw; rm %s** aus. Bei *printing = cups* und wenn Samba mit libcups kompiliert wurde, wird jeder manuell eingestellte Druckbefehl ignoriert!

17.4.1.6 Eigene Druckbefehle

Nachdem das Spoolen eines Druckauftrags an einen Dienst beendet ist, führt Samba den Druckbefehl in print command mit Hilfe eines *system()*-Aufrufs aus, um die Spool-Datei zu verarbeiten. Normalerweise übergibt der angegebene Befehl die Spool-Datei an das Drucksubsystem des Hosts. Aber das muss nicht zwingend der Fall sein. Möglicherweise entfernt das Drucksubsystem die Spool-Datei nicht von sich aus. Was immer Sie also

angeben, Sie sollten sich vergewissern, dass die Spool-Datei nach ihrer Bearbeitung gelöscht wird.

Bei den traditionellen Druckmethoden ist es kein Problem, eigene Druckbefehle anzugeben. Wenn Sie jedoch keine eigenen Druckbefehle erstellen möchten, sollten Sie sich gut mit den standardmäßig eingebauten Befehlen auskennen, die Samba für jedes Drucksubsystem verwendet (siehe Tabelle 17.1)(((automatischen Verweis setzen))). Bei allen in den vorherigen Absätzen aufgelisteten Befehlen sehen Sie Parameter der Form *%X*. Dies sind so genannte *Makros* bzw. Abkürzungen, die als Platzhalter für die Namen von echten Objekten verwendet werden. Zu dem Zeitpunkt, wenn ein Befehl mit einem solchen Platzhalter ausgeführt wird, fügt Samba den passenden Wert automatisch ein. Druckbefehle können mit allen Makro-Ersetzungen von Samba umgehen. Was das Drucken angeht, so sind folgende von besonderer Bedeutung:

- *%s, %f* — der Pfad zum Spool-Dateinamen
- *%p* — der passende Druckername
- *%J* — Der vom Client übermittelte Auftragsname
- *%c* — die Anzahl der gedruckten Seiten des gespoolten Auftrags (falls bekannt)
- *%z* — die Größe des gespoolten Druckauftrags (in Bytes)

Im Druckbefehl muss mindestens einmal der Parameter *%s* oder *%f* vorkommen. Der Parameter *%p* ist optional. Falls kein Druckername angegeben wird, wird *%p* heimlich aus dem Druckbefehl entfernt. In dem Fall wird der Auftrag an den Standarddrucker geschickt.

Falls er im Abschnitt *[global]* angegeben ist, wird der Druckbefehl für alle druckbaren Dienste verwendet, für die kein eigener Druckbefehl angegeben ist. Sollte es weder einen Druckbefehl für einen druckbaren Dienst noch einen globalen Druckbefehl geben, werden Spool-Dateien zwar erzeugt, aber nicht bearbeitet! Vor allem werden Druckdateien dann nicht gelöscht und verbrauchen Platz auf der Festplatte.

Auf manchen UNIX-Systemen kann möglicherweise nicht gedruckt werden, wenn das Konto „*nobody*“ verwendet wird. Falls das passiert, können Sie ein alternatives Gast-Konto erstellen und ihm Druckrechte zuweisen. Dieses Gast-Konto richten Sie im Abschnitt *[global]* mit dem Parameter *guest account* ein.

Sie können ziemlich komplexe Druckbefehle erstellen. Sie müssen sich klarmachen, dass Druckbefehle lediglich an eine UNIX-Shell weitergegeben werden. Die Shell vermag die enthaltenen Umgebungsvariablen wie üblich zu erweitern. (Die Syntax zum Einbinden einer UNIX-Umgebungsvariable *$variable* in einen Samba-Druckbefehl lautet *%$variable*.) Folgendes Beispiel für einen funktionierenden Wert von print command trägt den Druckauftrag in die Logdatei `/tmp/print.log` ein, druckt die Datei und löscht sie anschließend. In Shell-Skripten dient das Semikolon „;“ üblicherweise als Trennzeichen zwischen Befehlen:

```
        print command = echo Drucken von %s >> \
 /tmp/print.log; lpr -P %p %s; rm %s
```

Je nachdem, wie Sie auf Ihrem System Dateien normalerweise drucken, müssen Sie dieses Beispiel stark abwandeln, um zu Ihrem Befehl zu gelangen. Der Vorgabewert des Parameters print command variiert je nach Einstellung des Parameters printing. Ein weiteres Beispiel lautet:

```
print command = /usr/local/samba/bin/myprintscript %p %s
```

17.5 Die Weiterentwicklung des Druckens seit Samba-2.2

Vor Samba-2.2.x war die Unterstützung von Druckerservern bei Windows-Clients auf *LanMan*-Druckaufrufe beschränkt. Dies ist die gleiche Protokollebene, wie sie auch Windows 9x/Me-PCs bei der Freigabe von Druckern bieten. Ab dem Release 2.2.0 begann Samba damit, die nativen Druckmechanismen von Windows NT zu unterstützen. Diese sind mit Hilfe von *MS-RPC* (RPC = *Remote Procedure Calls*) implementiert. MS-RPCs verwenden beim Drucken immer *SPOOLSS* als benannten Kanal.

Durch die neue Unterstützung von SPOOLSS ergibt sich unter anderem folgende zusätzliche Funktionalität:

- Unterstützung beim Herunterladen von Druckertreiberdateien auf Windows 95/98/NT/2000-Clients bei Bedarf (*Point'n'Print*)
- Hochladen von Druckertreibern mit dem *Assistenten für die Druckerinstallation* (APW) von Windows NT oder den Imprints <`http://imprints.sourceforge.net/`>-Werkzeugen
- Unterstützung der nativen MS-RPC-Druckaufrufe wie StartDocPrinter, EnumJobs(), usw. (siehe die MSDN-Dokumentation <`http://msdn.microsoft.com/`> für weitere Informationen zur Druck-API von Win32)
- Unterstützung von *Access Control Lists* (ACL) auf Druckern in NT
- Verbesserte Unterstützung der Manipulation von Druckerschlangen durch Verwendung von internen Datenbanken für Informationen zu gespoolten Aufträgen (implementiert durch verschiedene `*.tdb`-Dateien)

Ein Vorteil einer Aufrüstung ist der, dass Samba-3 in der Lage ist, seine Drucker über Active Directory (oder LDAP) zu veröffentlichen.

Es existiert ein fundamentaler Unterschied zwischen Druckerservern unter MS Windows NT und der Arbeitsweise von Samba. Windows NT erlaubt die Installation lokaler Drucker, die nicht freigegeben sind. Dies ist ein Überbleibsel dessen, dass jeder Windows NT-Rechner (Server oder Client) von einem Benutzer als Workstation benutzt werden kann. Samba veröffentlicht alle Drucker, die verfügbar gemacht werden - entweder standardmäßig oder durch eine spezielle Deklaration mit druckerspezifischen Freigaben.

Windows NT/200x/XP Professional-Clients müssen die Standard-SMB-Druckerfreigabe nicht benutzen. Sie können direkt auf jedem Drucker eines anderen Windows NT-Hosts drucken, indem Sie MS-RPC benutzen. Das setzt natürlich voraus, dass der Client die nötigen Rechte auf dem entfernten Host hat, der den Drucker zur Verfügung stellt. Die Standardrechte, die Windows NT an einen Drucker zuweist, ergeben die Druckrechte der wohlbekannten Gruppe *Everyone*. (Ältere Clients der Sorte Windows 9x/Me können nur auf freigegebenen Druckern drucken).

17.5.1 Point'n'Print-Client-Treiber auf Samba-Servern

Darüber, was das alles bedeutet, herrscht große Verwirrung. Oft wird die Frage gestellt: „*Müssen Druckertreiber auf einem Samba-Host installiert sein oder nicht, um von Windows-Clients aus drucken zu können?*“ Die Antwort darauf lautet: nein, das ist nicht notwendig.

Natürlich können Windows NT/2000-Clients auch ihren APW laufen lassen, um Treiber *lokal* zu installieren (die sich dann mit einer Samba-basierten Druckerschlange verbinden können). Die gleiche Methode wird auch von Windows 9x/Me-Clients verwendet. (Ein *Fehler* in Samba 2.2.0 führt jedoch dazu, dass auf Windows NT/2000-Clients verlangt wird, dass der Samba-Server über einen für den Drucker gültigen Treiber verfügt. In Samba 2.2.1 wurde das korrigiert).

Eine neue Möglichkeit ist es jedoch, die Druckertreiber im Abschnitt *[print$]* in der Freigabe des Samba-Servers zu installieren, und sehr bequem ist es ebenfalls. Dann wird der Treiber für *alle* Clients (inklusive 95/98/ME) installiert, wenn sie sich zum ersten Mal mit dieser Druckerfreigabe verbinden. Das *Hochladen* oder *Ablegen* des Treibers in dieser *[print$]*-Freigabe sowie die folgende Bindung dieses Treibers an eine vorhandene Samba-Druckerfreigabe kann mit verschiedenen Mitteln erreicht werden:

- Ausführen des *APW* auf einem NT/200x/XP Professional-Client (das funktioniert nicht auf 95/98/ME-Clients)
- Verwenden der *Imprints*-Werkzeuge
- Verwenden der Kommandozeilenwerkzeuge *smbclient* und *rpcclient*
- Verwenden von *cupsaddsmb* (funktioniert nur beim CUPS-Drucksystem, nicht bei LPR/LPD, LPRng usw.)

Diese hochgeladenen Treiber verwendet Samba in keiner Weise dazu, die gespoolten Dateien zu bearbeiten. Diese Treiber werden ausschließlich von den Clients benutzt, die sie mit dem von Samba unterstützten „*Point'n'Print*“-Mechanismus heruntergeladen und installiert haben. Die Clients verwenden diese Treiber dazu, Druckdateien in dem Format zu erzeugen, das der Drucker (oder das UNIX-Drucksystem) benötigt. Von Samba erhaltene Druckdateien werden an das UNIX-Drucksystem weitergeleitet, das für die gesamte weitere Bearbeitung zuständig ist.

17.5.2 Der veraltete Abschnitt [printer$]

In Samba-Versionen vor 2.2 konnte eine Freigabe namens *[printer$]* verwendet werden. Dieser Name wurde von dem gleichnamigen Dienst übernommen, der von Windows 9x/Me-Clients erzeugt wird, die sich einen Drucker teilen. Windows 9x/Me-Druckerserver verfügen immer über einen Dienst namens *[printer$]*, der einen nur lesenden Zugang (ohne Passwort) zum Herunterladen von Druckertreibern bietet. Allerdings erlaubte Sambas erste Implementation einen Parameter namens *printer driver location* pro Freigabe. Dieser gab den Ort der Treiberdateien für diesen Drucker an. Ein anderer Parameter namens *printer driver* bot die Möglichkeit, einen Namen für den Druckertreiber anzugeben, der an den Client übergeben wird.

Diese Parameter, inklusive *printer driver file*, wurden nun entfernt und können in Samba-3-Installationen nicht mehr verwendet werden. Der Freigabename *[print$]* wird

nun für den Ort von herunterladbaren Druckertreibern benutzt. Er wird von dem Dienst *[print$]* übernommen, der von Windows NT-PCs erstellt wird, wenn sie sich einen Drucker teilen. Windows NT-Druckerserver verfügen immer über einen *[print$]*-Dienst, der Lese- und Schreibzugriff bietet (im Kontext seiner ACLs), um das Herunter- und Hochladen von Druckertreibern zu unterstützen. Das heißt nicht, dass Windows 9x/Me-Clients ignoriert werden. Diese können die Samba-Unterstützung der Freigabe *[print$]* ganz normal benutzen.

17.5.3 Erstellen der Freigabe [print$]

Um das Hoch- und Herunterladen von Druckertreiberdateien zu unterstützen, müssen Sie zunächst eine Dateifreigabe namens *[print$]* konfigurieren. Der öffentliche Name dieser Freigabe wird fest in den MS Windows-Clients codiert. Er kann nicht geändert werden, weil Windows-Clients so programmiert sind, dass sie nach einem Dienst mit exakt diesem Namen suchen, wenn Sie Druckertreiberdateien erhalten möchten.

Sie sollten die Serverdatei so modifizieren, dass Sie die globalen Parameter hinzufügen und die Dateifreigabe *[print$]* erstellen (natürlich sind einige der Parameterwerte, z.B. path beliebig gewählt und sollten durch die für Ihre Site passenden Werte ersetzt werden; siehe nächstes Beispiel).

Beispiel 17.5.1. Beispiel für [print\$]

```
[global]
# Mitglieder der Gruppe ntadmin sollten Treiber hinzufügen und
# Druckereigenschaften einstellen können. root ist implizit immer ein 'printer admin'.
        printer admin = @ntadmin
...

[printers]
...

[print$]
        comment = Druckertreiber-Download-Bereich
        path = /etc/samba/drivers
        browseable = yes
        guest ok = yes
        read only = yes
        write list = @ntadmin, root
```

Natürlich müssen Sie auch sicherstellen, dass das Verzeichnis mit dem Parameterwert path im UNIX-Dateisystem existiert.

17.5.4 Parameter im Abschnitt [print$]

[print$] ist ein besonderer Abschnitt in `smb.conf`. Er enthält Einstellungen, die relevant sind für potenziell herunterzuladende Druckertreiber und wird von Windows-Clients bei der

lokalen Installation von Druckertreibern verwendet. Folgende Parameter werden in diesem Freigabeabschnitt oft benötigt:

comment = Druckertreiber Download-Bereich Der Kommentar erscheint neben dem Freigabenamen, wenn er in der Freigabeliste aufgeführt wird (normalerweise werden Windows-Clients ihn nicht sehen, aber er erscheint auch oben in der Ausgabe des Befehls **smbclient -L sambaserver**).

path = /etc/samba/printers Dies ist der Pfad zu dem Ort, an dem die Windows-Druckertreiber aufbewahrt werden, aus der Sicht von UNIX.

browseable = no Macht die Freigabe *[print$]* für Clients aus der **Netzwerkumgebung** unsichtbar. Allerdings können Sie sie weiterhin von jedem beliebigen Client aus mounten, indem Sie den Befehl **net use g:\\sambaserver\print$** in einer DOS-Shell oder den Menüeintrag **Netzlaufwerk verbinden ...** im Windows Explorer verwenden.

guest ok = yes Gibt allen Gastbenutzern nur Lesezugriff auf diese Freigabe. Eventuell besteht die Möglichkeit, Druckertreiber auf Clients herunterzuladen und zu installieren. Ob der Parameter *guest ok = yes* notwendig ist, hängt davon ab, wie Ihre Site konfiguriert ist. Verfügen die Benutzer auf jeden Fall über ein Konto auf dem Samba-Host, so ist das kein Problem.

> ANMERKUNG
>
>
>
> Falls all Ihre Windows NT-Benutzer garantiert vom Samba-Server authentifiziert werden können (z.B. wenn Samba eine Authentifizierung mittels eines NT-Domainservers vornimmt und der Benutzer vom Domänencontroller beim Anmelden an eine Windows NT-Sitzung bereits validiert wurde), so ist kein Gastzugang notwendig. Wenn Sie natürlich in der Umgebung einer Arbeitsgruppe einfach nur drucken möchten, ohne sich um dumme Konten und Sicherheitsfragen zu kümmern, dann konfigurieren Sie die Freigabe so, dass sie einen Gastzugriff erlaubt. Eventuell sollten Sie sich überlegen, im Abschnitt *[global]* auch map to guest = Bad User hinzuzufügen. Vorher sollten Sie aber verstanden haben, was dieser Parameter bewirkt.

read only = yes Da wir nicht möchten, dass jeder Treiberdateien hochladen (oder sogar Treibereinstellungen ändern) kann, haben wir diese Freigabe als nicht schreibbar markiert.

write list = @ntadmin, root In der vorherigen Einstellung wurde *[print$]* nur lesbar

gemacht, damit wir auch den Eintrag *write list* erstellen konnten. UNIX-Gruppen werden mit einem führenden „@"-Zeichen angegeben. Die hier aufgeführten Benutzer verfügen über Schreibrechte (eine Ausnahme zu den Nur-Lese-Rechten für die Allgemeinheit), die sie für die Aktualisierung von Dateien in der Freigabe benötigen. Normalerweise werden Sie hier nur Benutzerkonten von Administratoren auflisten wollen. Prüfen Sie die Rechte im Dateisystem, um sicherzugehen, dass diese Konten Dateien in die Freigabe kopieren dürfen. Falls dies ein von root verschiedenes Konto ist, sollte das Konto im globalen Parameter printer admin erwähnt werden (siehe auch die Manpage zu `smb.conf` für weitere Informationen zur Konfiguration von Dateifreigaben).

17.5.5 Das Freigabeverzeichnis [print$]

Damit ein Windows NT-Druckerserver das Herunterladen von Druckertreibern für Clients von mehreren Architekturen unterstützen kann, müssen Sie mehrere Unterverzeichnisse für den Dienst *[print$]* erstellen (d.h. das UNIX-Verzeichnis mit dem Namen des Parameters path). Diese entsprechen den unterstützten Client-Architekturen. Samba verwendet dieses Modell ebenfalls. Genau wie der Name der Freigabe *[print$]* selbst müssen die Unterverzeichnisse genau die unten aufgeführten Namen haben (für Architekturen, die Sie nicht unterstützen müssen, können Sie die entsprechenden Unterverzeichnisse weglassen).

Erstellen Sie daher für jede Architektur, die Sie unterstützen möchten, einen Verzeichnisbaum unter der Freigabe *[print$]* wie folgt:

```
[print$]--+
          |--W32X86           # enthaelt Treiber fuer Windows NT x86
          |--WIN40            # enthaelt Treiber fuer Windows 95/98
          |--W32ALPHA         # enthaelt Treiber fuer Windows NT Alpha_AXP
          |--W32MIPS          # enthaelt Treiber fuer Windows NT R4000
          |--W32PPC           # enthaelt Treiber fuer Windows NT PowerPC
```

Erforderliche Rechte

Um einen neuen Treiber zu Ihrem Samba-Host hinzuzufügen, muss eine von zwei Bedingungen erfüllt sein:

- Das Konto, mit dem die Verbindung zum Samba-Host erfolgt, muss eine UID mit dem Wert 0 haben (d.h. root sein).
- Das Konto, mit dem die Verbindung zum Samba-Host erfolgt, muss in der Liste *printer admin* vorkommen.

Natürlich muss das Konto für die Verbindung außerdem Schreibrechte haben, um Dateien in die Unterverzeichnisse von *[print$]* einzufügen. Denken Sie daran, dass alle Dateifreigaben per Voreinstellung auf „*nur lesend*" gesetzt sind.

Nachdem Sie den erforderlichen Dienst *[print$]* samt zugehörigen Unterverzeichnissen erstellt haben, können Sie zu einer Windows NT 4.0/200x/XP-Client-Workstation gehen. Öffnen Sie dort die **Netzwerkumgebung** oder **Meine Netzwerkverbindungen**, und finden Sie den Samba-Host. Wenn Sie den Server gefunden haben, navigieren Sie zu dessen Ordner **Drucker und Faxgeräte**. Nun sollten Sie eine erste Liste von Druckern sehen, die den Druckerfreigaben entspricht, die auf Ihrem Samba-Host definiert sind.

17.6 Treiber in [print$] installieren

Haben Sie die Freigabe *[print$]* in `smb.conf` erfolgreich erstellt und haben Sie Samba dazu gebracht, seine Datei `smb.conf` neu zu lesen? Gut. Aber noch sind Sie nicht so weit, dass Sie Ihre neuen Möglichkeiten nutzen können. Noch müssen die Client-Treiberdateien in dieser Freigabe installiert werden. Bis jetzt ist es nur eine leere Freigabe. Leider reicht es nicht aus, die Treiberdateien einfach hineinzukopieren. Sie müssen korrekt installiert werden, damit in den internen Samba-Datenbanken für jeden Treiber entsprechende Einträge existieren und Samba die korrekten Treiber zur Verfügung stellen kann, wenn sie von MS Windows-Clients angefordert werden. Und das ist, gelinge gesagt, ein bischen haarig. Wir besprechen nun zwei alternative Möglichkeiten, die Treiber in *[print$]* zu installieren:

- Mit dem Kommandozeilen-Samba-Utility **rpcclient** und verschiedenen Unterbefehlen davon (hier: **adddriver** und **setdriver**) auf beliebigen UNIX-Workstations
- Mit Hilfe der GUI (**Druckereigenschaften** und des **Assistenten für die Druckerinstallation**) auf einer beliebigen Windows NT/200x/XP-Client-Workstation

Die zweite Möglichkeit ist wahrscheinlich die einfachere (auch dann, wenn der Vorgang zu Beginn ein wenig merkwürdig erscheinen mag).

17.6.1 Treiberinstallation mit dem Assistenten für die Druckerinstallation

Zu Beginn ist für die Druckerliste im Ordner **Drucker** des Samba-Hosts kein echter Druckertreiber mit den Druckern verbunden, wenn Sie mit einem Client-Explorer auf diesen Ordner zugreifen. Per Voreinstellung ist der Name dieses Treibers auf einen Nullstring gesetzt. Das muss nun geändert werden. Dabei wird uns der auf NT/2000/XP-Clients laufende lokale **Assistent für die Druckerinstallation** (APW) helfen.

Die Installation eines gültigen Druckertreibers ist nicht so einfach. Sie müssen versuchen, die Druckereigenschaften des Druckers zu sehen, dem Sie die Treiber zuordnen möchten. Öffnen Sie den Windows Explorer, öffnen Sie die **Netzwerkumgebung**, finden Sie den Samba-Host, öffnen Sie den Samba-Ordner **Drucker**, führen Sie einen Rechtsklick auf auf dem Drucker-Icon aus, und wählen Sie **Eigenschaften...** aus. Damit versuchen Sie, die Drucker- und Treibereigenschaften für eine Schlange anzuschauen, für die ein solcher `NULL`-Treiber voreingestellt ist. Das führt zu folgender Fehlermeldung:

Die Geräteeinstellungen können nicht angezeigt werden. Der Treiber für den angegebenen Drucker ist nicht installiert. (((??? Device settings cannot be displayed. The driver for the specified printer is not installed, only spooler properties will be displayed. Do you want to install the driver now?)))

Klicken Sie nicht auf **Ja**! Klicken Sie stattdessen im Fehlerdialogfeld auf **Nein**. Erst jetzt erhalten Sie ein Fenster mit den Druckereigenschaften. Von hier aus können wir nun überlegen, wie wir dem Drucker einen Treiber zuordnen wollen. Dabei haben Sie folgende Möglichkeiten:

- Wählen Sie einen Treiber aus der Pop-Up-Liste der installierten Treiber aus. Zu Beginn ist diese Liste leer.
- Klicken Sie auf **Neuer Treiber ...**, um einen neuen Druckertreiber zu installieren (daraufhin wird der APW gestartet).

Nachdem der APW gestartet worden ist, ist die Prozedur genau die gleiche wie jene, die Sie von Windows her kennen (wir nehmen hier an, dass Sie mit der Installation von Druckertreibern unter Windows NT vertraut sind). Vergewissern Sie sich, dass Ihre Verbindung tatsächlich als Benutzer mit printer admin-Privilegien eingerichtet ist (wenn Sie daran zweifeln, überprüfen Sie es mit **smbstatus**). Wenn Sie Druckertreiber für andere Betriebssysteme als Windows NT x86 installieren möchten, müssen Sie im Dialogfeld **Druckereigenschaften** den Reiter **Freigabe** verwenden.

Wenn Sie eine Verbindung unter einem Administrator- (oder root-)Konto hergestellt haben (wie durch den Parameter printer admin angegeben wird), dürfen Sie auch andere Druckereigenschaften wie ACLs und Vorgabewerte für Geräteeigenschaften in diesem Dialogfeld ändern. Was die Vorgabewerte von Geräteeigenschaften angeht, sollten Sie die Ratschläge befolgen, die im Abschnitt Druckertreiber installieren mit **rpcclient** gegebenen werden.

17.6.2 Druckertreiber installieren mit rpcclient

Die zweite Möglichkeit, Druckertreiber in *[print$]* zu installieren und als gültige Treiber einzurichten, besteht darin, die UNIX-Kommandozeile zu benutzen. Dazu gehören vier verschiedene Schritte:

1. Verschaffen Sie sich Information über die benötigten Treiberdateien, und besorgen Sie sich diese Dateien.
2. Legen Sie die Treiberdateien in die korrekten Unterverzeichnisse der Freigabe *[print$]* (eventuell mit dem Befehl **smbclient**).
3. Führen Sie das Kommandozeilen-Utility **rpcclient** mit dem Unterbefehl **adddriver** einmal aus.
4. Führen Sie **rpcclient** ein zweites Mal mit dem Unterbefehl **setdriver** aus.

In den folgenden Abschnitten erhalten Sie detaillierte Hinweise zu jedem einzelnen dieser Schritte.

17.6.2.1 Identifizieren von Treiberdateien

Um die Treiberdateien zu finden, haben Sie zwei Möglichkeiten. Sie können den Inhalt der Treiber-CD-ROM durchsuchen, die mit Ihrem Drucker geliefert wurde. Sehen Sie sich die `*.inf`-Dateien auf der CD-ROM an. Das ist manchmal nicht möglich, weil die `*.inf`-Dateien eventuell fehlen. Leider haben die Hersteller angefangen, ihre eigenen Installationsprogramme zu benutzen. Diese Installationspakete liegen oft in irgendeinem Archivformat für die

Windows-Plattform vor. Außerdem werden die Dateien während der Installation manchmal auch umbenannt. Leider wird es dadurch extrem schwierig, die benötigten Treiberdateien zu identifizieren.

In dem Fall steht Ihnen nur die zweite Möglichkeit zur Verfügung. Installieren Sie den Treiber lokal auf einem Windows-Client, und finden Sie heraus, welche Dateinamen und -pfade er nach dieser Installation benutzt. (Dieses Vorgehen müssen Sie für jede zu unterstützende Client-Plattform wiederholen. An dieser Stelle zeigen wir das nur für die Plattform W32X86, ein Name, der von Microsoft für alle Windows NT/200x/XP-Clients verwendet wird.)

Eine gute Methode zum Aufspüren der Treiberdateien besteht darin, aus dem Dialogfeld **Eigenschaften** des Treibers (Reiter **Allgemein**) eine Testseite auszudrucken. Wenn Sie dann in der Druckausgabe nach der Liste der Treiberdateien suchen, werden Sie feststellen, dass Windows (und Samba) folgende Dateien verwenden: **Treiberdatei**, **Datendatei**, **Konfig.-Datei**, **Hilfedatei** und (optional) **Abhängige Treiberdateien** (bei Windows NT kann das leicht anders sein). Für die weiteren Schritte müssen Sie sich alle Dateinamen notieren.

Eine andere Methode zum schnellen Testen der Treiberdateinamen und entsprechenden Pfade steht mit dem Utility **rpcclient** zur Verfügung. Starten Sie es mit **enumdrivers** oder mit dem Unterbefehl **getdriver**, die beide auf der Informationsebene `3` liegen. Im folgenden Beispiel ist *TURBO_XP* der Name eines Windows-PCs (in diesem Fall war es ein Laptop mit Windows XP Professional). Ich habe den Treiber lokal auf TURBO_XP installiert, und zwar von einem Samba-Server namens `KDE-BITSHOP`. Wir könnten eine interaktive **rpcclient**-Sitzung ausführen, wobei wir einen **rpcclient** />-Prompt bekämen und dort die Unterbefehle eingeben würden. Dies überlasse ich Ihnen, da es eine gute Übung ist. Im Moment benutzen wir **rpcclient** mit dem Parameter `-c`, um eine einzelne Unterbefehlszeile auszuführen, und sind dann fertig. Diese Methode würden Sie benutzen, wenn Sie Skripten erstellen möchten, um den Vorgang für eine große Anzahl von Druckern und Treibern zu automatisieren. Beachten Sie die verschiedenen Anführungszeichen, mit denen unterschiedliche Leerzeichen zwischen einzelnen Worten respektiert werden:

```
root# rpcclient -U'Danka%xxxx' -c \
   'getdriver "Heidelberg Digimaster 9110 (PS)" 3' TURBO_XP
cmd = getdriver "Heidelberg Digimaster 9110 (PS)" 3

[Windows NT x86]
Printer Driver Info 3:
  Version: [2]
  Driver Name: [Heidelberg Digimaster 9110 (PS)]
  Architecture: [Windows NT x86]
  Driver Path: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\HDNIS01_de.DLL]
  Datafile: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\Hddm91c1_de.ppd]
  Configfile: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\HDNIS01U_de.DLL]
  Helpfile: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\HDNIS01U_de.HLP]

  Dependentfiles: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\Hddm91c1_de.DLL]
  Dependentfiles: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\Hddm91c1_de.INI]
  Dependentfiles: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\Hddm91c1_de.dat]
  Dependentfiles: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\Hddm91c1_de.cat]
```

```
Dependentfiles: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\Hddm91c1_de.def]
Dependentfiles: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\Hddm91c1_de.hre]
Dependentfiles: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\Hddm91c1_de.vnd]
Dependentfiles: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\Hddm91c1_de.hlp]
Dependentfiles: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\HDNIS01Aux.dll]
Dependentfiles: [C:\WINNT\System32\spool\DRIVERS\W32X86\2\HDNIS01_de.NTF]

Monitorname: []
Defaultdatatype: []
```

Vielleicht bemerken Sie, dass dieser Treiber eine ziemlich große Anzahl von Dateien in der Kategorie **Dependentfiles** hat (es gibt aber auch schlimmere Fälle). Außerdem ist hier seltsamerweise **Driver File** mit **Driver Path** markiert. Wir haben noch keine Unterstützung für die so genannte WIN40-Architektur installiert. Dieser Name wird von Microsoft für die Plattformen Windows 9x/Me verwendet. Wenn wir diese unterstützen möchten, müssen wir auf einem Windows-PC die Treiberdateien für Windows 9x/Me zusätzlich zu denen für W32X86, d.h. für Windows NT/2000/XP-Clients installieren. Dieser PC kann ebenfalls die Windows 9x/Me-Treiber beherbergen, selbst dann, wenn er unter Windows NT, 2000 oder XP läuft.

Da die Freigabe *[print$]* normalerweise über die **Netzwerkumgebung** erreichbar ist, können Sie vom Windows Explorer aus auch die UNC-Notation benutzen, um darin herumzustochern. Die Windows 9x/Me-Treiberdateien werden im Unterverzeichnis `0` des Verzeichnisses `WIN40` abgelegt. Der vollständige Pfad für den Zugriff darauf lautet dann `\\WINDOWSHOST\print$\WIN40\0\`.

ANMERKUNG

Neuere Treiber auf Windows 2000 und Windows XP werden im Unterverzeichnis „*3*“ statt „*2*“ installiert. Version 2 der Treiber, wie sie in Windows NT benutzt werden, liefen vorher im Kernel-Modus. Mit Windows 2000 hat sich das verändert. Zwar kann es weiterhin die Treiber im Kernel-Modus benutzen (falls das vom Administrator erlaubt ist), aber der native Modus für seine Druckertreiber ist die Ausführung im User-Modus. Dafür sind speziell entworfene Treiber notwendig. Diese Art von Treibern werden im Unterverzeichnis „*3*“ installiert.

17.6.2.2 Treiberdateien aus [print$]-Freigaben von Windows-Clients erhalten

Nun müssen wir alle im vorherigen Schritt gefundenen Treiberdateien zusammentragen. Wo bekommen wir die aber her? Nun, warum nehmen wir sie nicht einfach vom gleichen PC und der gleichen Freigabe *[print$]*, die wir in unserem letzten Schritt untersucht haben, um die Dateien zu finden? Dazu können wir **smbclient** verwenden. Wir benutzen dabei die Pfade und Namen, die uns **getdriver** verraten hat. Das folgende Listing ist leicht editiert,

damit es durch zusätzliche Umbrüche leichter lesbar wird:

```
root# smbclient //TURBO_XP/print\$ -U'Danka%xxxx' \
   -c 'cd W32X86/2;mget HD*_de.* hd*ppd Hd*_de.* Hddm*dll HDN*Aux.DLL'

added interface ip=10.160.51.60 bcast=10.160.51.255 nmask=255.255.252.0
Got a positive name query response from 10.160.50.8 ( 10.160.50.8 )
Domain=[DEVELOPMENT] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
Get file Hddm91c1_de.ABD? n
Get file Hddm91c1_de.def? y
getting file \W32X86\2\Hddm91c1_de.def of size 428 as Hddm91c1_de.def
Get file Hddm91c1_de.DLL? y
getting file \W32X86\2\Hddm91c1_de.DLL of size 876544 as Hddm91c1_de.DLL
[...]
```

Nach der Ausführung dieses Befehls befinden sich die Dateien in unserem aktuellen lokalen Verzeichnis. Vermutlich haben Sie bemerkt, dass wir dieses Mal mehrere durch Semikola getrennte Befehle mit dem Parameter `-c` übergeben haben. Das bewirkt, dass auf dem entfernten Windows-Server alle Befehle nacheinander ausgeführt werden, bevor smbclient wieder beendet wird.

Vergessen Sie nicht, diese Prozedur für die WIN40-Architektur zu wiederholen, falls Sie Windows 9x/Me/XP-Clients unterstützen müssen. Denken Sie dabei auch daran, dass die Dateien für diese Architekturen sich im Unterverzeichnis `WIN40/0/` befinden. Wenn das erledigt ist, können wir **smbclient ... put** starten, um die gesammelten Dateien in der Freigabe *[print$]* des Samba-Servers zu speichern.

17.6.2.3 Treiberdateien in [print$] installieren

Nun werden wir die Treiberdateien in der Freigabe *[print$]* platzieren. Denken Sie daran, dass der UNIX-Pfad zu dieser Freigabe zuvor in Ihren eigenen Worten definiert wurde, die hier aber fehlen. Außerdem haben Sie Unterverzeichnisse für die verschiedenen zu unterstützenden Arten von Windows-Clients angelegt. Wenn wir annehmen, dass Ihre Freigabe *[print$]* auf den UNIX-Pfad `/etc/samba/drivers/` abgebildet wird, dann sollten Ihre Treiberdateien an folgende Orte gelangen:

- Für alle Windows NT-, 2000- und XP-Clients nach `/etc/samba/drivers/W32X86/`, aber (noch) nicht in das Verzeichnis `2`
- Für alle Windows 95-, 98- und ME-Clients nach `/etc/samba/drivers/WIN40/` aber (noch) nicht in das Verzeichnis `0`

Wieder benutzen wir smbclient für die Übertragung der Treiberdateien über das Netzwerk. Wir geben die gleichen Dateien und Pfade an, die wir bei der Ausführung von **getdriver** im Vergleich mit der Originalinstallation von *Windows* erhalten haben. Nun aber werden wir die Dateien in der Freigabe *[print$]* eines *Samba/UNIX*-Druckerservers speichern.

```
root# smbclient //SAMBA-CUPS/print\$ -U'root%xxxx' -c \
```

```
  'cd W32X86; put HDNIS01_de.DLL; \
  put Hddm91c1_de.ppd; put HDNIS01U_de.DLL;        \
  put HDNIS01U_de.HLP; put Hddm91c1_de.DLL;        \
  put Hddm91c1_de.INI; put Hddm91c1KMMin.DLL;      \
  put Hddm91c1_de.dat; put Hddm91c1_de.dat;        \
  put Hddm91c1_de.def; put Hddm91c1_de.hre;        \
  put Hddm91c1_de.vnd; put Hddm91c1_de.hlp;        \
  put Hddm91c1_de_reg.HLP; put HDNIS01Aux.dll;     \
  put HDNIS01_de.NTF'

added interface ip=10.160.51.60 bcast=10.160.51.255 nmask=255.255.252.0
Got a positive name query response from 10.160.51.162 ( 10.160.51.162 )
Domain=[CUPS-PRINT] OS=[UNIX] Server=[Samba 2.2.7a]
putting file HDNIS01_de.DLL as \W32X86\HDNIS01_de.DLL
putting file Hddm91c1_de.ppd as \W32X86\Hddm91c1_de.ppd
putting file HDNIS01U_de.DLL as \W32X86\HDNIS01U_de.DLL
putting file HDNIS01U_de.HLP as \W32X86\HDNIS01U_de.HLP
putting file Hddm91c1_de.DLL as \W32X86\Hddm91c1_de.DLL
putting file Hddm91c1_de.INI as \W32X86\Hddm91c1_de.INI
putting file Hddm91c1KMMin.DLL as \W32X86\Hddm91c1KMMin.DLL
putting file Hddm91c1_de.dat as \W32X86\Hddm91c1_de.dat
putting file Hddm91c1_de.dat as \W32X86\Hddm91c1_de.dat
putting file Hddm91c1_de.def as \W32X86\Hddm91c1_de.def
putting file Hddm91c1_de.hre as \W32X86\Hddm91c1_de.hre
putting file Hddm91c1_de.vnd as \W32X86\Hddm91c1_de.vnd
putting file Hddm91c1_de.hlp as \W32X86\Hddm91c1_de.hlp
putting file Hddm91c1_de_reg.HLP as \W32X86\Hddm91c1_de_reg.HLP
putting file HDNIS01Aux.dll as \W32X86\HDNIS01Aux.dll
putting file HDNIS01_de.NTF as \W32X86\HDNIS01_de.NTF
```

Puh, das war viel zu tippen! Die meisten Treiber sind wesentlich kleiner — viele haben sogar nur drei generische PostScript-Treiberdateien plus eine PPD-Datei. Obwohl wir die Dateien aus dem Unterverzeichnis `2` des Verzeichnisses `W32X86` von der Windows-Kiste geholt haben, platzieren wie sie (vorläufig) nicht in das gleiche Unterverzeichnis der Samba-Kiste. Dieses Umkopieren wird automatisch vom Befehl **adddriver** erledigt, den wir gleich ausführen werden (und vergessen Sie ebenfalls nicht, auch die Dateien für die Windows 9x/Me-Architektur in das Unterverzeichnis `WIN40/` zu legen, falls Sie diese brauchen sollten).

17.6.2.4 Bestätigen der Treiberinstallation mit smbclient

Im Moment überprüfen wir nur, dass unsere Dateien vorhanden sind. Das kann ebenfalls mit dem Befehl **smbclient** bewerkstelligt werden (aber Sie können sich natürlich auch mit SSH anmelden und das mit einem Zugriff über eine UNIX-Shell erledigen):

```
root# smbclient //SAMBA-CUPS/print\$ -U 'root%xxxx' \
   -c 'cd W32X86; pwd; dir; cd 2; pwd; dir'
```

```
 added interface ip=10.160.51.60 bcast=10.160.51.255 nmask=255.255.252.0
Got a positive name query response from 10.160.51.162 ( 10.160.51.162 )
Domain=[CUPS-PRINT] OS=[UNIX] Server=[Samba 2.2.8a]

Current directory is \\SAMBA-CUPS\print$\W32X86\
.                                   D        0  Sun May  4 03:56:35 2003
..                                  D        0  Thu Apr 10 23:47:40 2003
2                                    D        0  Sun May  4 03:56:18 2003
HDNIS01Aux.dll                       A    15356  Sun May  4 03:58:59 2003
Hddm91c1KMMin.DLL                    A    46966  Sun May  4 03:58:59 2003
HDNIS01_de.DLL                       A   434400  Sun May  4 03:58:59 2003
HDNIS01_de.NTF                       A   790404  Sun May  4 03:56:35 2003
Hddm91c1_de.DLL                      A   876544  Sun May  4 03:58:59 2003
Hddm91c1_de.INI                      A      101  Sun May  4 03:58:59 2003
Hddm91c1_de.dat                      A     5044  Sun May  4 03:58:59 2003
Hddm91c1_de.def                      A      428  Sun May  4 03:58:59 2003
Hddm91c1_de.hlp                      A    37699  Sun May  4 03:58:59 2003
Hddm91c1_de.hre                      A   323584  Sun May  4 03:58:59 2003
Hddm91c1_de.ppd                      A    26373  Sun May  4 03:58:59 2003
Hddm91c1_de.vnd                      A    45056  Sun May  4 03:58:59 2003
HDNIS01U_de.DLL                      A   165888  Sun May  4 03:58:59 2003
HDNIS01U_de.HLP                      A    19770  Sun May  4 03:58:59 2003
Hddm91c1_de_reg.HLP                  A   228417  Sun May  4 03:58:59 2003
              40976 blocks of size 262144. 709 blocks available

Current directory is \\SAMBA-CUPS\print$\W32X86\2\
.                                   D        0  Sun May  4 03:56:18 2003
..                                  D        0  Sun May  4 03:56:35 2003
ADOBEPS5.DLL                         A   434400  Sat May  3 23:18:45 2003
laserjet4.ppd                        A     9639  Thu Apr 24 01:05:32 2003
ADOBEPSU.DLL                         A   109568  Sat May  3 23:18:45 2003
ADOBEPSU.HLP                         A    18082  Sat May  3 23:18:45 2003
PDFcreator2.PPD                      A    15746  Sun Apr 20 22:24:07 2003
              40976 blocks of size 262144. 709 blocks available
```

Beachten Sie, dass in dem Unterverzeichnis 2 schon Treiberdateien vorhanden sind (vermutlich aus einer früheren Installation). Nachdem die Dateien für den neuen Treiber ebenfalls dort sind, sind es noch einige wenige Schritte, bevor Sie sie auf einem Client benutzen können. Das einzige, was Sie nun tun könnten, ist, sie von einem Client zu bekommen, so wie Sie auch normale Dateien von einer Dateifreigabe bekommen würden, indem Sie print$ im Windows Explorer öffnen. Aber dabei würden sie nicht per Point'n'Print installiert. Der Grund ist folgender: Samba weiß noch nicht, dass diese Dateien etwas Besonderes sind, nämlich *Druckertreiberdateien*, und es weiß nicht, zu welcher Druckerschlange bzw. zu welchen Druckerschlangen diese Treiberdateien gehören.

17.6.2.5 Ausführen von rpcclient mit adddriver

Als Nächstes müssen Sie Samba sagen, dass es sich um eine spezielle Sorte von Dateien handelt, die Sie gerade in der Freigabe *[print$]* hochgeladen haben. Das tun Sie mit dem Befehl **adddriver**. Dieser bringt Samba dazu, die Treiberdateien in seiner internen TDB-Datenbank zu registrieren. Der folgende Befehl und seine Ausgabe wurden wieder zwecks besserer Lesbarkeit editiert:

```
root# rpcclient -Uroot%xxxx -c 'adddriver "Windows NT x86" \
  "dm9110:HDNIS01_de.DLL: \
  Hddm91c1_de.ppd:HDNIS01U_de.DLL:HDNIS01U_de.HLP:   \
  NULL:RAW:Hddm91c1_de.DLL,Hddm91c1_de.INI,          \
  Hddm91c1_de.dat,Hddm91c1_de.def,Hddm91c1_de.hre,   \
  Hddm91c1_de.vnd,Hddm91c1_de.hlp,Hddm91c1KMMin.DLL, \
  HDNIS01Aux.dll,HDNIS01_de.NTF,                     \
  Hddm91c1_de_reg.HLP' SAMBA-CUPS

cmd = adddriver "Windows NT x86" \
  "dm9110:HDNIS01_de.DLL:Hddm91c1_de.ppd:HDNIS01U_de.DLL:   \
  HDNIS01U_de.HLP:NULL:RAW:Hddm91c1_de.DLL,Hddm91c1_de.INI, \
  Hddm91c1_de.dat,Hddm91c1_de.def,Hddm91c1_de.hre,          \
  Hddm91c1_de.vnd,Hddm91c1_de.hlp,Hddm91c1KMMin.DLL,        \
  HDNIS01Aux.dll,HDNIS01_de.NTF,Hddm91c1_de_reg.HLP"

Printer Driver dm9110 successfully installed.
```

Nach diesem Schritt sollte der Treiber von Samba auf dem Druckerserver erkannt werden. Bei der Eingabe des Befehls müssen Sie sehr vorsichtig sein. Vertauschen Sie nicht die Reihenfolge der Felder. Manche Änderungen würden zu der Fehlermeldung `NT_STATUS_UNSUCCESSFUL` führen. Diese Fehler sind offensichtlich. Bei anderen Änderungen werden die Treiberdateien erfolgreich installiert, aber ohne dass der Treiber selbst funktioniert. Also passen Sie auf! Hinweise zur Syntax des Befehls **adddriver** finden Sie in der Manpage. Das Kapitel über das Drucken mit CUPS enthält eine detailliertere Beschreibung, falls Sie eine solche brauchen sollten.

17.6.2.6 Ende von adddriver überprüfen

Ein Hinweis darauf, dass Samba die Dateien als Treiberdateien erkennt, ist die Meldung `successfully installed`. Ein weiterer ist die Tatsache, dass unsere Dateien vom Befehl **adddriver** in das Unterverzeichnis `2` verschoben wurden. Das können Sie erneut mit **smbclient** überprüfen:

```
root# smbclient //SAMBA-CUPS/print\$ -Uroot%xx \
   -c 'cd W32X86;dir;pwd;cd 2;dir;pwd'
 added interface ip=10.160.51.162 bcast=10.160.51.255 nmask=255.255.252.0
 Domain=[CUPS-PRINT] OS=[UNIX] Server=[Samba 2.2.7a]
```

```
Current directory is \\SAMBA-CUPS\print$\W32X86\
.                                   D        0  Sun May  4 04:32:48 2003
..                                  D        0  Thu Apr 10 23:47:40 2003
2                                    D        0  Sun May  4 04:32:48 2003
                40976 blocks of size 262144. 731 blocks available

Current directory is \\SAMBA-CUPS\print$\W32X86\2\
.                                   D        0  Sun May  4 04:32:48 2003
..                                  D        0  Sun May  4 04:32:48 2003
DigiMaster.PPD                       A   148336  Thu Apr 24 01:07:00 2003
ADOBEPS5.DLL                         A   434400  Sat May  3 23:18:45 2003
laserjet4.ppd                        A     9639  Thu Apr 24 01:05:32 2003
ADOBEPSU.DLL                         A   109568  Sat May  3 23:18:45 2003
ADOBEPSU.HLP                         A    18082  Sat May  3 23:18:45 2003
PDFcreator2.PPD                      A    15746  Sun Apr 20 22:24:07 2003
HDNIS01Aux.dll                       A    15356  Sun May  4 04:32:18 2003
Hddm91c1KMMin.DLL                    A    46966  Sun May  4 04:32:18 2003
HDNIS01_de.DLL                       A   434400  Sun May  4 04:32:18 2003
HDNIS01_de.NTF                       A   790404  Sun May  4 04:32:18 2003
Hddm91c1_de.DLL                      A   876544  Sun May  4 04:32:18 2003
Hddm91c1_de.INI                      A      101  Sun May  4 04:32:18 2003
Hddm91c1_de.dat                      A     5044  Sun May  4 04:32:18 2003
Hddm91c1_de.def                      A      428  Sun May  4 04:32:18 2003
Hddm91c1_de.hlp                      A    37699  Sun May  4 04:32:18 2003
Hddm91c1_de.hre                      A   323584  Sun May  4 04:32:18 2003
Hddm91c1_de.ppd                      A    26373  Sun May  4 04:32:18 2003
Hddm91c1_de.vnd                      A    45056  Sun May  4 04:32:18 2003
HDNIS01U_de.DLL                      A   165888  Sun May  4 04:32:18 2003
HDNIS01U_de.HLP                      A    19770  Sun May  4 04:32:18 2003
Hddm91c1_de_reg.HLP                  A   228417  Sun May  4 04:32:18 2003
                40976 blocks of size 262144. 731 blocks available
```

Sie können auch noch prüfen, ob der Zeitstempel der Druck-TDB-Dateien nun aktualisiert ist (und eventuell, ob deren Dateigröße zugenommen hat).

17.6.2.7 Treibererkennung in Samba überprüfen

Nun sollte der Treiber in Samba registriert sein. Das können wir leicht nachprüfen und werden es auch gleich tun. Allerdings ist dieser Treiber noch nicht mit einem bestimmten Drucker verbunden. Den Status der Treiberdateien können wir auf mindestens dreierlei Weise überprüfen:

- Stöbern Sie auf einem beliebigen Windows-Client in der Netzwerkumgebung, finden Sie dort den Samba-Host, und öffnen Sie den Samba-Ordner **Drucker und Faxgeräte**. Wählen Sie ein beliebiges Drucker-Icon, und führen Sie einen Rechtsklick aus, um die Drucker-**Eigenschaften** zu wählen. Klicken Sie auf den Reiter **Erweitert**. Dort ist ein

Feld, das den Treiber für diesen Drucker angibt. In einem Drop-Down-Menü können Sie diesen Treiber ändern (achten Sie aber darauf, das nicht unabsichtlich zu tun). Mit dieser Liste haben Sie eine Übersicht aller Treiber, die Samba kennt. Ihr neuer Treiber sollte nun auch darunter sein. (Dabei sieht jede Sorte von Client nur die Liste für ihre eigene Architektur. Wenn Sie nicht alle Treiber für alle Plattformen installiert haben, sieht die Liste unterschiedlich aus, je nachdem, ob Sie sie unter Windows95/98/ME oder Windows NT/2000/XP anschauen.)

- Stöbern Sie auf einem Windows 200x/XP-Client (nicht Windows NT) die **Netzwerkumgebung** auf, suchen Sie den Samba-Server, öffnen Sie den Ordner **Drucker** des Servers, und führen Sie einen Rechtsklick auf dem weißen Hintergrund aus (ohne markierten Drucker). Wählen Sie **Server-Eigenschaften** im Menü aus. Unter dem Reiter **Treiber** werden Sie den neuen Treiber aufgelistet sehen. In dieser Ansicht können Sie auch die Liste der zu diesem Treiber gehörenden Dateien inspizieren. (Das funktioniert nicht unter Windows NT, sondern nur unter Windows 2000 und Windows XP; Windows NT verfügt nicht über den Reiter **Treiber**.) Eine alternative und wesentlich schnellere Methode, dieses Dialogfeld unter Windows 2000/XP zu starten, besteht darin, in einer DOS-Shell Folgendes einzugeben (natürlich müssen Sie *SAMBA-CUPS* durch den Namen Ihres Samba-Servers ersetzen):

  ```
  rundll32 printui.dll,PrintUIEntry /s /t2 /n\\SAMBA-CUPS
  ```

- Führen Sie unter einem UNIX-Prompt folgenden Befehl (oder eine Variante davon) aus, wobei *SAMBA-CUPS* der Name des Samba-Hosts ist und xxxx für das aktuelle an root zugewiesene Samba-Passwort steht:

  ```
  rpcclient -U'root%xxxx' -c 'enumdrivers' SAMBA-CUPS
  ```

  Dann sehen Sie eine Liste aller Samba bekannten Treiber. Darunter sollte auch ihr neuer sein. Er wird allerdings nur unter der Überschrift *[Windows NT x86]* aufgeführt, nicht unter *[Windows 4.0]*, weil Sie diesen Teil nicht installiert haben. Oder haben Sie es doch getan? In unserem Beispiel hat der Treiber den Namen `dm9110`. Beachten Sie, dass in der dritten Spalte die anderen installierten Treiber doppelt erscheinen: je einmal für jede unterstützte Architektur. Unser neuer Treiber erscheint nur unter Windows NT 4.0 oder 2000. Um ihn auch unter Windows 95, 98 und ME zu sehen, müssen Sie die gesamte Prozedur mit der WIN40-Architektur und dem WIN40-Unterverzeichnis wiederholen.

17.6.2.8 Spezifische Flexibilität von Treibernamen

Sie können den Treiber nennen, wie Sie möchten. Wenn Sie den Schritt **adddriver** mit den gleichen Dateien wie vorher, aber mit einem anderen Treibernamen wiederholen, funktioniert es genauso:

```
root# rpcclient -Uroot%xxxx         \
  -c 'adddriver "Windows NT x86"                    \
  "mydrivername:HDNIS01_de.DLL:             \
  Hddm91c1_de.ppd:HDNIS01U_de.DLL:HDNIS01U_de.HLP:   \
  NULL:RAW:Hddm91c1_de.DLL,Hddm91c1_de.INI,          \
```

```
  Hddm91c1_de.dat,Hddm91c1_de.def,Hddm91c1_de.hre,   \
  Hddm91c1_de.vnd,Hddm91c1_de.hlp,Hddm91c1KMMin.DLL, \
  HDNIS01Aux.dll,HDNIS01_de.NTF,Hddm91c1_de_reg.HLP' SAMBA-CUPS


cmd = adddriver "Windows NT x86" \
 "mydrivername:HDNIS01_de.DLL:Hddm91c1_de.ppd:HDNIS01U_de.DLL:\
  HDNIS01U_de.HLP:NULL:RAW:Hddm91c1_de.DLL,Hddm91c1_de.INI,          \
  Hddm91c1_de.dat,Hddm91c1_de.def,Hddm91c1_de.hre,                   \
  Hddm91c1_de.vnd,Hddm91c1_de.hlp,Hddm91c1KMMin.DLL,                 \
  HDNIS01Aux.dll,HDNIS01_de.NTF,Hddm91c1_de_reg.HLP"

Printer Driver mydrivername successfully installed.
```

Diesen Treiber können Sie mit einer beliebigen Druckerschlange verbinden (allerdings sind Sie dafür verantwortlich, Treiber mit Schlangen zu verbinden, die in Hinblick auf die anvisierten Drucker auch Sinn machen). Den Befehl **rpcclient adddriver** können Sie nicht mehrfach wiederholen. Bei jeder Ausführung werden die Dateien verbraucht, die Sie in die Freigabe *[print$]* gelegt, d.h. in die entsprechenden Unterverzeichnisse verschoben haben. Daher müssen Sie vor jedem **rpcclient ... adddriver**-Befehl den Befehl **smbclient ... put** ausführen.

17.6.2.9 Ausführen von rpcclient mit setdriver

Samba muss darüber Bescheid wissen, welcher Treiber zu welchem Drucker gehört. Erstellen Sie eine Zuordnung der Treiber zu ihren Druckern, und speichern Sie diese Information in Sambas Speicher, den TDB-Dateien. Genau dies bewerkstelligt der Befehl **rpcclient setdriver**:

```
root# rpcclient -U'root%xxxx' -c 'setdriver dm9110 mydrivername' SAMBA-CUPS
 cmd = setdriver dm9110 mydrivername

Successfully set dm9110 to driver mydrivername.
```

Ähm, nein, das wollte ich eigentlich gar nicht tun. Also noch einmal, jetzt mit dem beabsichtigten Namen:

```
root# rpcclient -U'root%xxxx' -c 'setdriver dm9110 dm9110' SAMBA-CUPS
 cmd = setdriver dm9110 dm9110
Successfully set dm9110 to driver dm9110.
```

Die Syntax des Befehls lautet:

```
rpcclient -U'root%sambapassword' -c 'setdriver printername \
```

```
drivername' SAMBA-Hostname.
```

Nun haben wir den größten Teil der Arbeit erledigt, aber noch nicht alles.

ANMERKUNG

Der Befehl **setdriver** ist nur dann erfolgreich, wenn Samba den Drucker bereits kennt. Ein Fehler in 2.2.x verhindert, dass Samba frisch installierte Drucker erkennt. Dort müssen Sie Samba neu starten oder zumindest ein HUP-Signal an alle laufenden smbd-Prozesse schicken, um dieses Problem zu umgehen: `kill -HUP 'pidof smbd'`.

17.7 Installationsvorgang bei Client-Treibern

Wie Don Quixote schon sagte, geht Probieren über Studieren: „*The proof of the pudding is in the eating.*“ Die Prüfung unserer Einstellungen besteht im erfolgreichen Drucken. Installieren wir also den Druckertreiber auf den Client-PCs. Das ist nicht ganz so einfach, wie es erscheinen mag. Lesen Sie also weiter.

17.7.1 Treiberinstallation auf dem ersten Client

Besonders wichtig ist die Installation auf dem ersten Client-PC (für jede Architektur einzeln). Sobald diese korrekt erfolgt ist, sind alle weiteren Clients leicht einzurichten und sollten keine weitere Aufmerksamkeit benötigen. Es folgt nun eine Beschreibung der Prozedur, die für das erste Mal empfohlenen wird. Sie arbeiten nun auf einer Client-Workstation. Sie sollten sicherstellen, dass Ihre Verbindung nicht unabsichtlich unter dem *ungeeigneten Benutzer „nobody“* erfolgt. Geben Sie nun in einer DOS-Shell Folgendes ein:

```
net use \\SAMBA-SERVER\print$ /user:root
```

Ersetzen Sie, falls erforderlich, root durch einen anderen gültigen printer admin-Benutzer, der in der Definition angegeben ist. Sollten Sie bereits als anderer Benutzer verbunden sein, so erhalten Sie eine Fehlermeldung. Eine einfache Möglichkeit, diese Verbindung loszuwerden, gibt es nicht, da Windows anscheinend das Konzept des Abmeldens von einer Freigabeverbindung nicht kennt (verwechseln Sie das nicht mit dem Abmelden von der lokalen Workstation, was eine völlig andere Sache ist). Unter Windows NT/2K können Sie ein Abmelden von allen smb/cifs-Verbindungen erzwingen, indem Sie den Dienst „*workstation*“ neu starten. Sie können versuchen, alle Dateiexplorer- und Internet Explorer-Fenster unter Windows zu schließen. Als letzte Möglichkeit müssen Sie möglicherweise einen Neustart durchführen. Vergewissern Sie sich, dass nicht automatisch eine Verbindung neu hergestellt wird. Es ist eventuell leichter, zu einer anderen Workstation zu gehen und es von dort auszuprobieren. Wenn Sie sicher sind, dass Sie als Benutzer printer admin verbunden

sind (das können Sie in Samba mit dem Befehl **smbstatus** prüfen), führen Sie folgende Schritte auf der Windows-Workstation aus:

1. Öffnen Sie die **Netzwerkumgebung**.
2. Gehen Sie zum Samba-Server.
3. Öffnen Sie dessen Ordner **Drucker und Faxgeräte**.
4. Wählen Sie den Drucker, und führen Sie einen Rechtsklick darauf aus.
5. Wählen Sie **Verbinden** (unter Windows NT4/200x heißt es eventuell **Installieren**).

Ein neuer Drucker (namens *printername* auf dem Samba-Server) sollte nun in Ihrem *lokalen* Druckerordner erschienen sein (prüfen Sie das mit **Start** – **Einstellungen** – **Systemsteuerung** – **Drucker und Faxgeräte**).

Sehr wahrscheinlich möchten Sie nun versuchen, eine Testseite auszudrucken. Schließlich können Sie nun die Druckereigenschaften öffnen, und unter dem Reiter **Allgemein** gibt es einen Knopf genau dafür. Aber sehr wahrscheinlich würden Sie eine Fehlermeldung namens Unable to print Test Page erhalten. Der Grund könnte sein, dass noch kein gültiger Device-Modus für den Drucker gesetzt ist oder dass der Satz an „*Druckertreiberdaten*“ noch immer unvollständig ist.

Sie müssen sicherstellen, dass für den Drucker ein gültiger *Device-Modus* gesetzt ist. Wir wollen nun erklären, was das bedeutet.

17.7.2 Device-Modus auf neuen Druckern setzen

Damit ein Drucker wirklich von einem Windows NT/200x/XP-Client benutzt werden kann, muss er über Folgendes verfügen:

- Einen gültigen *Device-Modus*, der von dem Druckertreiber generiert wird (und Dinge wie die Papiergröße, -ausrichtung und Duplex-Einstellungen definiert)
- Einen kompletten Satz an *Druckertreiberdaten*, der vom Treiber generiert wird

Ist eine dieser Angaben unvollständig, so können die Clients bestenfalls eine suboptimale Ausgabe produzieren. Im schlimmsten Fall kommt unlesbarer Müll oder gar nichts aus dem Drucker. Oder er produziert eine Unmenge Fehlermeldungen beim Versuch, etwas auszudrucken. Samba speichert die genannten Werte sowie alle druckrelevanten Informationen in seinen internen TDB-Datenbankdateien (`ntprinters.tdb`, `ntdrivers.tdb`, `printing.tdb` und `ntforms.tdb`).

Wofür stehen diese beiden Begriffe? Im Grunde genommen stellen der Device-Modus und der Satz an Druckertreiberdaten eine Ansammlung von Einstellungen für alle Eigenschaften einer Druckerschlange dar, die mit vernünftigen Anfangswerten versehen sind. Device-Modi und Druckertreiberdaten sollten auf dem Druckerserver (dem Samba-Host) vernünftige Anfangswerte haben, damit die Clients sie sofort benutzen können. Wie aber stellen wir diese vernünftigen Werte ein? Das kann man dadurch erreichen, dass man auf die Treiber von einem entfernten NT- (oder 200x/XP-) Client aus zugreift, was in den folgenden Abschnitten beschrieben wird.

Sie sollten sich darüber im Klaren sein, dass ein gültiger Device-Modus nur von einem printer admin oder von root eingestellt werden kann (aus offensichtlichen Gründen). Device-Modi können nur durch die Ausführung des Druckertreiberprogramms selbst korrekt eingestellt werden. Da Samba den Treibercode für diese Win32-Plattform nicht ausführen kann, setzt es dieses Feld anfangs auf NULL (was für Clients kein gültiger verwendbarer Wert ist). Zum Glück generieren die meisten Treiber die Druckertreiberdaten automatisch, die beim Hochladen auf die Freigabe *[print$]* mit APW oder **rpcclient** benötigt werden.

Das Generieren und Einstellen eines ersten gültigen Device-Modus erfordert jedoch einige Kitzelei auf dem Client, um ihn auf dem Samba-Server zu setzen. Die einfachste Art, das zu tun, besteht darin, die Papierausrichtung auf dem Drucker des Servers zu ändern. Dabei wird genug vom Druckertreiberprogramm auf dem Client ausgeführt, damit der gewünschte Effekt eintritt und der neue Device-Modus auf unserem Samba-Server eingestellt wird. Dazu können Sie die Seite **Druckereigenschaften** von Windows NT/200x/XP auf einem Windows-Client benutzen:

1. Stöbern Sie in der **Netzwerkumgebung.**
2. Finden Sie den Samba-Server.
3. Öffnen Sie den Ordner **Drucker und Faxgeräte** des Samba-Servers.
4. Selektieren Sie den entsprechenden freigegebenen Drucker.
5. Führen Sie einen Rechtsklick auf dem Drucker aus (wenn Sie die Beschreibung im letzten Abschnitt befolgt haben, sind Sie eventuell schon hier).
6. Selektieren Sie unten im Kontextmenü **Eigenschaften** (wenn das Menü weiter oben noch den Eintrag **Verbinden** zeigt, müssen Sie zuerst darauf klicken, um die Treiberinstallation so durchzuführen, wie im letzten Abschnitt gezeigt).
7. Klicken Sie auf den Reiter **Erweitert**, dann auf **Standardwerte**.
8. Ändern Sie die Seiteneinstellungen für **Hochformat** auf **Querformat** (und zurück).
9. Vergewissern Sie sich, dass Sie die Änderungen zwischen dem Umschalten der Seitenausrichtung auch anwenden, damit die Änderung auch wirksam wird.
10. Wenn Sie schon dabei sind, möchten Sie hier eventuell auch die gewünschten Druckvoreinstellungen setzen, die dann bei allen zukünftigen Treiberinstallationen auf den verbleibenden Clients angewendet werden.

Diese Prozedur hat das Druckertreiberprogramm auf der Client-Plattform ausgeführt und den korrekten Device-Modus an Samba zurückgegeben, das ihn nun in seinen TDB-Dateien gespeichert hat. Nachdem der Treiber einmal auf dem Client installiert ist, können Sie analoge Schritte befolgen und auf den *lokalen* Ordner **Drucker** ebenfalls zugreifen, sofern Sie ein printer admin-Benutzer von Samba sind. Von nun an sollte das Drucken wie erwartet funktionieren.

Samba verfügt auf der Serviceebene über einen Parameter namens *default devmode* zum Generieren eines Standard-Device-Modus für einen Drucker. Manche Treiber funktionieren gut mit Sambas Standardeigenschaften, andere können eventuell den Spooling-Dienst des Clients zum Absturz bringen. Daher sollten Sie diesen Parameter mit Vorsicht verwenden.

Es ist immer besser, den Client einen gültigen Device-Modus für den Drucker erstellen zu lassen und für Sie auf dem Server zu speichern.

17.7.3 Installation weiterer Client-Treiber

Jeder weiterer Treiber kann wie oben beschrieben installiert werden: im Netzwerk stöbern, den Ordner **Drucker** auf dem Samba-Server öffnen, auf **Drucker** rechts-klicken und **Verbinden...** auswählen. Sobald das fertig ist (es sollte nicht länger als ein paar Sekunden dauern, kann aber je nach Netzwerkverhältnissen auch eine Minute dauern), sollten Sie den neuen Drucker im lokalen Ordner **Drucker und Faxgeräte** Ihrer Client-Workstation finden.

Ihren lokalen Ordner **Drucker und Faxgeräte** können Sie auf Windows 200x/XP Professional-Workstations auch mit dem folgenden Befehl öffnen:

```
rundll32 shell32.dll,SHHelpShortcuts_RunDLL PrintersFolder
```

oder mit diesem Befehl auf Windows NT 4.0-Workstations:

```
rundll32 shell32.dll,Control_RunDLL MAIN.CPL @2
```

Sie können diese Befehle entweder in einer **DOS-Shell** eingeben oder im Feld **Ausführen...** des **Start**-Menüs.

17.7.4 Erste Client-Verbindung immer als root oder „*printer admin*“ herstellen

Nachdem Sie den Treiber auf dem Samba-Server installiert haben (in dessen Freigabe *[print$]*, sollten Sie immer sichergehen, dass Ihre erste Client-Installation korrekt beendet wurde. Machen Sie es sich zur Gewohnheit, die allererste Verbindung von einem Client als printer admin zu machen. Damit wird Folgendes garantiert:

- Ein erster gültiger *Device-Modus* wird tatsächlich initialisiert (siehe oben für erklärende Details).
- Die Standarddruckeinstellungen Ihres Druckers sind für alle weiteren Client-Installationen so, wie Sie es wünschen.

Tun Sie dies durch eine Änderung der Papierausrichtung auf Querformat, klicken Sie auf **Anwenden**, und machen Sie die Einstellung anschließend wieder rückgängig. Als Nächstes ändern Sie die anderen Einstellungen (Sie wollen z.B. die Standardpapiergröße nicht auf **Letter** setzen, wenn Sie immer **A4** benutzen, oder? Vielleicht möchten Sie den Drucker standardmäßig **duplex** drucken lassen usw.).

Probieren Sie folgenden Befehl beim Prompt einer Windows 200x/XP-DOS-Shell aus, um sich als root mit einem Samba-Drucker zu verbinden:

```
C:\> runas /netonly /user:root "rundll32 printui.dll,PrintUIEntry /p /t3 /n
   \\SAMBA-SERVER\printername"
```

Sie werden nun nach dem Samba-Passwort von root gefragt. Geben Sie es ein, warten Sie einige Sekunden, klicken Sie auf **Standardwerte**, und fahren Sie mit der Einstellung

der Standardoptionen für Druckaufträge fort, die von allen Clients benutzt werden sollen. Alternativ zu root können Sie ein anderes Mitglied von printer admin angeben.

Nun haben alle anderen Benutzer, die den Treiber auf die gleiche Weise (genannt „*Point'n'Print*“) herunterladen und installieren, dieselben voreingestellten Werte dafür. Wenn Sie diesen Schritt auslassen, wird Ihre Telefonauskunft eine Menge Anrufe von Ihren Benutzern bekommen, aber vielleicht lieben Sie es ja auch, mit diesen zu sprechen.

17.8 Andere Fallstricke

Ihr Treiber ist installiert und bereit für die Installation per Point'n'Print durch die Clients. Vielleicht haben Sie versucht, ihn auf Ihrem ersten Client-Rechner herunterzuladen und zu benutzen, aber warten Sie noch. Stellen wir erst sicher, dass Sie mit ein paar Tipps und Tricks vertraut sind, die eventuell hilfreich für Sie sein werden. Nehmen wir z.B. an, Sie haben auf dem Drucker keine Standardwerte eingestellt, wie es Ihnen in den vorherigen Absätzen geraten wurde. Ihre Benutzer beklagen sich über verschiedene Probleme, z.B. „*Wir müssen für jeden Druckauftrag die Papiergröße von Letter auf A4 umstellen, und das wird nicht gespeichert.*“)

17.8.1 Standarddruckeroptionen für Client-Treiber einstellen

Der letzte Satz mag von einigen Benutzern und Admins mit gemischten Gefühlen betrachtet werden. Sie haben stundenlang gekämpft und es nicht geschafft, an einen Punkt zu kommen, an dem ihre Einstellungen anscheinend gespeichert werden. Es ist nicht deren Schuld. Das Verwirrende ist, dass Sie in dem Dialogfeld mit mehreren Reitern, das nach einem Rechtsklick auf dem Druckernamen und der Auswahl von **Eigenschaften** erscheint, zu zwei scheinbar identischen Dialogfeldern gelangen können, die beide behaupten, Ihnen zu helfen, Druckereigenschaften auf dreierlei Art einzustellen. Hier ist die definitive Antwort zu dieser FAQ über die Samba-Standarddruckereinstellungen:

„Ich kann für alle Benutzer von Windows 200x/XP keine Standarddruckoptionen einstellen und speichern. Warum nicht?“. Wie haben Sie es versucht? Ich wette, auf die falsche Art. (Aber es ist nicht leicht, das herauszufinden). Es gibt drei verschiedene Wege, auf denen Sie zu einem Dialogfeld gelangen, das scheinbar alles einstellt. Alle drei Dialogfelder sehen gleich aus, aber nur eines davon tut das, was Sie möchten. Um dies für alle Benutzer zu machen, müssen Sie Administrator oder Print Administrator sein. Auf folgende Weise kann ich es unter XP Professional reproduzieren:

A Der erste „*falsche*“ Weg:

1 Öffnen Sie den Ordner **Drucker**.

2 Führen Sie einen Rechtsklick auf dem Drucker aus (*entfernterdrucker(((Schreibweise okay so?))) auf cupshost*), und wählen Sie im Kontextmenü **Druckereinstellungen...** aus.

3 Sehen Sie sich dieses Dialogfeld genau an, und prägen Sie sich ein, wie es aussieht.

B Der zweite „*falsche*“ Weg: . . .

1 Öffnen Sie den Ordner **Drucker**.

2 Führen Sie einen Rechtsklick auf dem Drucker aus (*entfernterdrucker(((s.o.))) auf cupshost*), und wählen Sie im Kontextmenü **Einstellungen** aus.

3 Klicken Sie auf den Reiter **Allgemein** tab

4 Klicken Sie auf **Druckereigenschaften...**

5 Ein neues Dialogfeld wird geöffnet. Halten Sie es geöffnet, und gehen Sie zurück zu seinem Elterndialogfeld.

C Der dritte und korrekte Weg: (Sollten Sie das von Anfang an tun, führen Sie einfach die Schritte 1 und 2 aus der obigen zweiten Methode aus).

1 Klicken Sie auf den Reiter **Erweitert**. (Falls alles „*grau hinterlegt*“ ist, so sind Sie nicht als Benutzer mit ausreichenden Rechten angemeldet.)

2 Klicken Sie auf **Standardwerte**.

3 Klicken Sie auf einem beliebigen der beiden neuen Reiter auf den Button **Erweitert**.

4 Ein neues Dialogfeld wird geöffnet. Vergleichen Sie dieses mit dem anderen. Sehen Sie gleich aus, wenn Sie das eine aus „*B.5*“ mit dem aus „*A.3*“ vergleichen?

Sehen Sie irgendeinen Unterschied in den beiden Dialogfeldern? Ich auch nicht. Aber nur im letzten, zu dem Sie mit den Schritten C.1 bis 6 gelangt sind, werden Einstellungen permanent gespeichert und werden daher zu Vorgabewerten bei neuen Benutzern. Wenn Sie möchten, dass diese Vorgabewerte für alle Clients gleich sind, müssen Sie diese Schritte als Administrator (printer admin in `smb.conf`) ausführen, bevor ein Client den Treiber herunterlädt (später können die Clients ihre eigenen benutzerspezifischen Vorgabewerte mit Hilfe der obigen Prozeduren A oder B einstellen). Windows 200x/XP erlaubt benutzerspezifische Vorgabewerte und solche, die die Rechner vom Administrator erhalten, bevor die Benutzer ihre eigenen Werte einstellen. Die Dialogfelder, die diesen identisch aussehenden Dialogfeldern vorausgehen, unterscheiden sich geringfügig in den Namen ihrer Fenster: eines heißt `Default Print Values for Printer Foo on Server Bar`(((???))) (das ist das Fenster, das Sie benötigen), und ein anderes heißt „*`Print Settings for Printer Foo on Server Bar`*“(((???))). Zu letzterem gelangen Sie, wenn Sie auf den Drucker rechts-klicken und **Druckereinstellungen...** auswählen. Weil man Ihnen zur Zeit von Windows NT gesagt hat, Sie sollten dieses Fenster benutzen, ist es nur natürlich, es unter Windows 200x/XP genauso auszuprobieren. Man würde nicht im Traum daran denken, dass man nun einen anderen Weg gehen muss, um zu einem identisch aussehenden, aber funktional verschiedenen Dialogfeld zu gelangen, um Vorgabewerte für alle Benutzer zu setzen.

TIPP

Versuchen Sie (unter Windows 200x/XP), diesen Befehl auszuführen (als Benutzer mit den nötigen Rechten):

`rundll32 printui.dll,PrintUIEntry /p /t3 /n\\`*`SAMBA-SERVER\printersharename`*

Um den Reiter mit dem Knopf **Standardwerte** zu sehen (den Sie benötigen), führen Sie auch diesen Befehl aus:

`rundll32 printui.dll,PrintUIEntry /p /t0 /n\\`*`SAMBA-SERVER\printersharename`*

Um den Reiter mit dem Button **Printing Preferences** zu sehen (derjenige, der keine systemweiten Vorgabewerte setzt), können Sie die Befehle aus einer DOS-Shell oder mit **Start** -> **Ausführen** ausführen.

17.8.2 Unterstützung einer großen Anzahl von Druckern

Während der letzten Entwicklungsphase von Samba ist ein Problem aufgetaucht, das die Unterstützung beim Herunterladen von Treibern für Hunderte von Druckern betrifft. Den APW in Windows NT dafür zu benutzen ist, gelinde gesagt, ein wenig umständlich. Wenn Sie sich keine Sehnenscheidenentzündung allein von der Klick-Orgie bei der Druckerinstallation holen möchten, müssen Sie über ein nicht-interaktives Skript nachdenken.

Wenn mehr als ein Drucker den gleichen Treiber verwendet, kann man den Befehl **rpcclient setdriver** benutzen, um den mit einer Druckerschlage verbundenen Treiber zu setzen. Wenn der Treiber einmal nach *[print$]* hochgeladen und in den Drucker-TDBs registriert ist, kann er von mehreren Druckerschlangen verwendet werden. In diesem Fall müssen Sie nur den Unterbefehl **setprinter** von **rpcclient** bei jeder Schlange wiederholen (ohne, dass Sie **adddriver** wiederholt ausführen müssen). Das Folgende ist ein Beispiel dafür, wie man das machen kann:

```
root# rpcclient SAMBA-CUPS -U root%secret -c 'enumdrivers'
 cmd = enumdrivers

 [Windows NT x86]
 Printer Driver Info 1:
   Driver Name: [infotec  IS 2075 PCL 6]

 Printer Driver Info 1:
   Driver Name: [DANKA InfoStream]

 Printer Driver Info 1:
   Driver Name: [Heidelberg Digimaster 9110 (PS)]
```

```
 Printer Driver Info 1:
   Driver Name: [dm9110]

 Printer Driver Info 1:
   Driver Name: [mydrivername]

 [....]


root# rpcclient SAMBA-CUPS -U root%secret -c 'enumprinters'
 cmd = enumprinters
   flags:[0x800000]
   name:[\\SAMBA-CUPS\dm9110]
   description:[\\SAMBA-CUPS\dm9110,,110ppm HiVolume DANKA Stuttgart]
   comment:[110 ppm HiVolume DANKA Stuttgart]
 [....]


root# rpcclient SAMBA-CUPS -U root%secret -c \
  'setdriver dm9110 "Heidelberg Digimaster 9110 (PS)"'
 cmd = setdriver dm9110 Heidelberg Digimaster 9110 (PPD)
 Successfully set dm9110 to driver Heidelberg Digimaster 9110 (PS).


root# rpcclient SAMBA-CUPS -U root%secret -c 'enumprinters'
 cmd = enumprinters
   flags:[0x800000]
   name:[\\SAMBA-CUPS\dm9110]
   description:[\\SAMBA-CUPS\dm9110,Heidelberg Digimaster 9110 (PS),\
     110ppm HiVolume DANKA Stuttgart]
   comment:[110ppm HiVolume DANKA Stuttgart]
 [....]


root# rpcclient SAMBA-CUPS -U root%secret -c 'setdriver dm9110 mydrivername'
 cmd = setdriver dm9110 mydrivername
 Successfully set dm9110 to mydrivername.


root# rpcclient SAMBA-CUPS -U root%secret -c 'enumprinters'
 cmd = enumprinters
   flags:[0x800000]
   name:[\\SAMBA-CUPS\dm9110]
   description:[\\SAMBA-CUPS\dm9110,mydrivername,\
     110ppm HiVolume DANKA Stuttgart]
```

```
  comment:[110ppm HiVolume DANKA Stuttgart]
[....]
```

Es ist vielleicht nicht so einfach festzustellen, dass der erste Aufruf von **enumprinters** den Drucker „*dm9110*“ mit einem leeren String angezeigt hat, wo der Treiber aufgeführt sein sollte (zwischen den zwei Kommas im Beschreibungsfeld). Nachdem der Befehl **setdriver** ausgeführt wurde, ist alles in Ordnung.

17.8.3 Neue Drucker mit dem Windows NT-APW hinzufügen

Standardmäßig zeigt Samba im Ordner **Drucker** alle Druckerfreigaben an, die in `smb.conf` definiert sind. Außerdem befindet sich in diesem Ordner das Icon für den Assistent für die Druckerinstallation in Windows NT. Der APW wird nur dann gezeigt, wenn:

- Der verbundene Benutzer erfolgreich ein **OpenPrinterEx(\\server)** mit Administratorrechten, d.h. als root oder printer admin, ausführen kann.

> TIPP
>
>
>
> Versuchen Sie Folgendes beim Prompt einer DOS-Shell unter Windows 200x/XP:
>
> `runas /netonly /user:root rundll32 printui.dll,PrintUIEntry /p /t0 /n \\`*`SAMBA-SERVER\printersharename`*
>
> Klicken Sie auf **Druckereinstellungen**.

- ... die Einstellung show add printer wizard = yes enthält (das ist der Vorgabewert).

Der APW kann verschiedene Dinge erledigen:

- Einen Treiber auf der Freigabe *[print$]* von Samba hochladen.
- Einen hochgeladenen Treiber mit einer vorhandenen (noch treiberlosen) Druckerschlange verbinden.
- Den aktuell verwendeten Treiber für eine vorhandene Druckerschlange durch einen zuvor hochgeladenen Treiber ersetzen.
- Einen völlig neuen Drucker auf dem Samba-Host hinzufügen (nur in Verbindung mit einem funktionierenden add printer command. Ein entsprechendes delete printer command zum Entfernen von Einträgen aus dem Ordner **Drucker** wird eventuell auch angeboten).

Für den letzten Punkt, einen neuen Drucker hinzuzufügen, ist mehr Aufwand nötig als für die anderen. Um mit dem APW einen Drucker zu einem Samba-Server erfolgreich hinzufügen zu können, muss für add printer command ein Wert definiert sein. Das Programm muss den

Drucker mittels eines so genannten „*hooks*“ erfolgreich ins UNIX-Drucksystem einhängen (d.h. in die Dateien `/etc/printcap`, `/etc/cups/printers.conf` oder andere entsprechende Dateien) sowie in `smb.conf`, falls nötig.

Wenn Sie APW auf einem Client benutzen und die genannte Druckerfreigabe nicht existiert, wird smbd add printer command ausführen und versuchen, die neue Druckerfreigabe zu finden. Wenn die Freigabe weiterhin nicht definiert ist, wird ein Fehler namens Access Denied an den Client zurückgegeben. add printer command wird im Kontext des verbundenen Benutzers ausgeführt, was nicht notwendigerweise der von root ist. Mit map to guest = bad user wurden Sie vielleicht unabsichtlich mit den falschen Rechten verbunden. Sie sollten das mit dem Befehl **smbstatus** überprüfen.

17.8.4 Fehlermeldung: „*Cannot connect under a different Name*“

Wenn Sie erst einmal mit den falschen Angaben verbunden sind, gibt es keine andere Möglichkeit, die Situation zu ändern, als alle Explorer-Fenster zu schließen und vielleicht einen Neustart durchzuführen.

- Der Befehl **net use \\SAMBA-SERVER\sharename /user:root** gibt Ihnen folgende Fehlermeldung: „*Multiple connections to a server or a shared resource by the same user utilizing the several user names are not allowed. Disconnect all previous connections to the server, esp. the shared resource, and try again.*“
- Jeder Versuch einer „*Verbindung eines Netzwerklaufwerks*“ von `\\SAMBASERVER\print$` mit `z:` wird mit dieser hartnäckigen Meldung quittiert: „*This network folder is currently connected under different credentials (username and password). Disconnect first any existing connection to this network share in order to connect again under a different username and password*“.

Also beenden Sie alle Verbindungen. Sie versuchen es erneut. Wieder erhalten Sie die gleiche Meldung. Sie überprüfen die Einstellungen auf der Seite von Samba mit dem Befehl **smbstatus**. Ja, es gibt weitere Verbindungen. Sie terminieren sie alle. Der Client gibt Ihnen weiterhin die gleiche Fehlermeldung aus. Sie sehen sich die Datei smbd.log mit einem hohen Debug-Level an und versuchen eine neue Verbindung: die gleiche Fehlermeldung, aber keine einzige Zeile in der Log-Datei. Sie beginnen sich zu fragen, ob es überhaupt einen Verbindungsversuch gab. Sie führen **ethereal** und **tcpdump** aus, während Sie einen neuen Verbindungsversuch starten. Ergebnis: Kein einziges Byte wird übertragen. Windows gibt immer noch die Fehlermeldung aus. Sie schließen alle Explorer-Fenster und starten es neu. Sie versuchen eine Verbindung zu — und dieses Mal funktioniert es! Anscheinend speichert Windows irgendwo Verbindungsinformationen zwischen, ohne diese zu aktualisieren (und wenn Sie Pech haben, müssen Sie einen Neustart durchführen, um die Fehlermeldung loszuwerden).

Die einfachste Art, alle Verbindungen von Ihrem Client zu einem Server gewaltsam zu terminieren, besteht im Ausführen von:

```
C:\>  net use * /delete
```

Dadurch werden auch alle abgebildeten Laufwerke getrennt, so dass Sie neue Verbindungen nach Bedarf erstellen können.

17.8.5 Passen Sie beim Zusammenstellen von Treiberdateien auf

Sie müssen extrem vorsichtig ein, wenn Sie sich Notizen zu den Dateien machen, die zu einem bestimmten Treiber gehören. Verwechseln Sie nicht die Dateien für die Treiberversion „*0*“ (für Windows 9x/Me gehen diese nach `[print$]/WIN/0/`), Treiberversion 2 (Kernel-Modus-Treiber für Windows NT, die nach `[print$]/W32X86/2/` gehen und eventuell auch unter Windows 200x/XP benutzt werden können) und Treiberversion „*3*“ (Nicht-Kernel-Modus-Treiber unter `[print$]/W32X86/3/`, können nicht unter Windows NT benutzt werden). Diese verschiedenen Treiberversionen enthalten recht oft Dateien, die den gleichen Namen haben, aber sehr verschieden sind. Wenn Sie diese im Windows Explorer betrachten (Sie finden sie in `%WINDOWS%\system32\spool\drivers\W32X86\`), sehen Sie wahrscheinlich Namen in Großbuchstaben, während der Befehl **enumdrivers** aus Samba große und kleine oder nur kleine Buchstaben anzeigen würde. Daher ist es leicht, sie zu verwechseln. Wenn Sie sie manuell mit **rpcclient** und dessen Unterbefehlen installieren, bekommen Sie vielleicht nicht einmal eine Fehlermeldung. Erst bei der späteren Installation auf einem Client werden Sie Fehlermeldungen wie `This server has no appropriate driver for the printer` fnden.

Hier ist ein Beispiel. Sie sollten sich die verschiedenen Dateien sehr genau anschauen und ihre Namen und Schreibweise vergleichen, um die Unterschiede in der Zusammensetzung von Version 2 und 3 der zwei Sätze zu bemerken. Man beachte: Da Version 0 des Satzes 40 *`Dependentfiles`* enthielt, habe ich diese aus Platzgründen ausgelassen:

```
root# rpcclient -U 'Administrator%secret' -c 'enumdrivers 3' 10.160.50.8

 Printer Driver Info 3:
         Version: [3]
         Driver Name: [Canon iR8500 PS3]
         Architecture: [Windows NT x86]
         Driver Path: [\\10.160.50.8\print$\W32X86\3\cns3g.dll]
         Datafile: [\\10.160.50.8\print$\W32X86\3\iR8500sg.xpd]
         Configfile: [\\10.160.50.8\print$\W32X86\3\cns3gui.dll]
         Helpfile: [\\10.160.50.8\print$\W32X86\3\cns3g.hlp]

         Dependentfiles: [\\10.160.50.8\print$\W32X86\3\aucplmNT.dll]
         Dependentfiles: [\\10.160.50.8\print$\W32X86\3\ucs32p.dll]
         Dependentfiles: [\\10.160.50.8\print$\W32X86\3\tnl32.dll]
         Dependentfiles: [\\10.160.50.8\print$\W32X86\3\aussdrv.dll]
         Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cnspdc.dll]
         Dependentfiles: [\\10.160.50.8\print$\W32X86\3\aussapi.dat]
         Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cns3407.dll]
         Dependentfiles: [\\10.160.50.8\print$\W32X86\3\CnS3G.cnt]
         Dependentfiles: [\\10.160.50.8\print$\W32X86\3\NBAPI.DLL]
         Dependentfiles: [\\10.160.50.8\print$\W32X86\3\NBIPC.DLL]
```

```
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcview.exe]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcdspl.exe]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcedit.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcqm.exe]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcspl.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cfine32.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcr407.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\Cpcqm407.hlp]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcqm407.cnt]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cns3ggr.dll]

        Monitorname: []
        Defaultdatatype: []

Printer Driver Info 3:
        Version: [2]
        Driver Name: [Canon iR5000-6000 PS3]
        Architecture: [Windows NT x86]
        Driver Path: [\\10.160.50.8\print$\W32X86\2\cns3g.dll]
        Datafile: [\\10.160.50.8\print$\W32X86\2\IR5000sg.xpd]
        Configfile: [\\10.160.50.8\print$\W32X86\2\cns3gui.dll]
        Helpfile: [\\10.160.50.8\print$\W32X86\2\cns3g.hlp]

        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\AUCPLMNT.DLL]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\aussdrv.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\cnspdc.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\aussapi.dat]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\cns3407.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\CnS3G.cnt]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\NBAPI.DLL]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\NBIPC.DLL]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\cns3gum.dll]

        Monitorname: [CPCA Language Monitor2]
        Defaultdatatype: []
```

Wenn wir die Dateien der „*Version 2*“ und der „*Version 3*“ in verschiedene Textdateien schreiben und das Ergebnis vergleichen, erhalten wir folgendes Bild:

```
root# sdiff 2-files 3-files


 cns3g.dll                      cns3g.dll
 iR8500sg.xpd                   iR8500sg.xpd
 cns3gui.dll                    cns3gui.dll
 cns3g.hlp                      cns3g.hlp
```

```
AUCPLMNT.DLL                | aucplmNT.dll
                            > ucs32p.dll
                            > tnl32.dll
aussdrv.dll                   aussdrv.dll
cnspdc.dll                    cnspdc.dll
aussapi.dat                   aussapi.dat
cns3407.dll                   cns3407.dll
CnS3G.cnt                     CnS3G.cnt
NBAPI.DLL                     NBAPI.DLL
NBIPC.DLL                     NBIPC.DLL
cns3gum.dll                 | cpcview.exe
                            > cpcdspl.exe
                            > cpcqm.exe
                            > cpcspl.dll
                            > cfine32.dll
                            > cpcr407.dll
                            > Cpcqm407.hlp
                            > cpcqm407.cnt
                            > cns3ggr.dll
```

Lassen Sie sich nicht foppen! Treiberdateien mit identischen Namen für jede Version können sich inhaltlich unterscheiden, wie Sie aus diesem Größenvergleich erkennen können:

```
root# for i in cns3g.hlp cns3gui.dll cns3g.dll; do                  \
          smbclient //10.160.50.8/print\$ -U 'Administrator%xxxx' \
          -c "cd W32X86/3; dir $i; cd .. ; cd 2; dir $i";      \
        done

  CNS3G.HLP               A   122981  Thu May 30 02:31:00 2002
  CNS3G.HLP               A    99948  Thu May 30 02:31:00 2002

  CNS3GUI.DLL             A  1805824  Thu May 30 02:31:00 2002
  CNS3GUI.DLL             A  1785344  Thu May 30 02:31:00 2002

  CNS3G.DLL               A  1145088  Thu May 30 02:31:00 2002
  CNS3G.DLL               A    15872  Thu May 30 02:31:00 2002
```

In meinem Beispiel gab es sogar noch mehr Unterschiede, als hier gezeigt werden. Die Schlussfolgerung lautet: Sie müssen sehr vorsichtig sein, um die korrekten Treiberdateien für jede Treiberversion auszuwählen. Verlassen Sie sich nicht allein auf die Namen, und tauschen Sie keine Dateien aus, die zu verschiedenen Treiberversionen gehören!

17.8.6 Samba- und Drucker-Ports

Windows NT/2000-Druckerserver verbinden mit jedem Drucker einen Port. Diese haben normalerweise die Form `LPT1:`, `COM1:`, `FILE:` usw. Samba muss das Konzept von Ports, die mit einem Drucker verbunden sind, ebenfalls unterstützen. Standardmäßig existiert auf einem System nur ein Drucker-Port namens „*Samba Printer Port*“. Um zu drucken, braucht Samba einen solchen „*port*“ nicht wirklich, er wird lediglich von Windows-Clients benötigt. Diese bestehen darauf, dass man ihnen einen verfügbaren Port mitteilt, wenn sie danach fragen, sonst erhalten Sie von ihnen eine Fehlermeldung. Daher fingiert Samba die Port-Informationen, damit Windows-Clients glücklich sind.

Auch das Konzept des `Printer Poolings` wird intern von Samba nicht unterstützt. Beim Printer Pooling wird ein logischer Drucker mit mehreren Ports für eine Art Lastausgleich oder Überlauf verbunden.

Wenn Sie aus dem einen oder anderen Grunde mehrere Ports definiert haben müssen (meine Benutzer und mein Chef sollten nicht wissen, dass sie mit Samba arbeiten), konfigurieren Sie enumports command, mit dem ein externes Programm definiert werden kann, das eine Liste von Ports auf einem System generieren kann.

17.8.7 Wie Sie übliche Fehlkonfigurationen von Client-Treibern vermeiden

Nun können Sie also ausdrucken, aber es gibt weiterhin noch Probleme. Die meisten Druckaufträge werden prima ausgedruckt, einige werden aber gar nicht gedruckt. Manche Aufträge haben Probleme mit Fonts, die nicht gut aussehen. Manche Aufträge werden sehr schnell gedruckt, andere extrem langsam. Wir können es nicht gänzlich abhandeln, aber wir möchten Sie dazu ermuntern, den kurzen Absatz über „*Das Vermeiden von kritischen PostScript-Treiber-Einstellungen auf dem Client*“ in dem Kapitel über das Drucken mit CUPS zu lesen.

17.9 Das Tool-Set Imprints

Das Tool-Set namens Imprints bietet ein UNIX-Äquivalent des Assistenten für die Druckerinstallation von Windows NT. Vollständige Informationen dazu entnehmen Sie bitte der Website von Imprints <`http://imprints.sourceforge.net/`> wie auch der Dokumentation, die in der Quelldistribution von Imprints enthalten ist. Dieser Abschnitt enthält nur eine kurze Einführung zu den Möglichkeiten von Imprints.

Leider wird das Tool-Set Imprints nicht mehr weiter gepflegt. Seit Dezember 2000 sucht das Projekt einen neuen Leiter. Die wichtigsten Fähigkeiten dafür sind Perl-Kenntnisse und Interesse am Drucken auf Basis von MS-RPC in Samba. Wenn Sie sich freiwillig melden möchten, koordinieren Sie das bitte auf der technischen Mailingliste zu Samba. Das Tool-Set ist noch immer in einem benutzbaren Zustand, allerdings nur für eine Reihe älterer Druckermodelle, für die man vorbereitete Pakete benutzen kann. Wenn Imprints eine Zukunft haben soll, dann werden Pakete auch für aktuellere Drucker benötigt.

17.9.1 Was ist Imprints?

Imprints ist eine Sammlung von Werkzeugen, die folgende Ziele unterstützen:

- Bereitstellen einer zentralen Informationsstelle für Druckertreiberpakete zu Windows NT und 95/98
- Bereitstellen der notwendigen Werkzeuge zum Erstellen von Imprints-Druckertreiberpaketen
- Bereitstellen eines Installationsprogramms, das Druckertreiber von einer zentralen Internet- (oder Intranet-)Datenbank eines Imprints-Servers erhält und sie auf entfernten Samba- und Windows NT4-Druckerservern installiert

17.9.2 Druckertreiberpakete erstellen

Die Erstellung von Druckertreiberpaketen darzustellen übersteigt den Rahmen dieses Kapitels bei weitem (weitere Information darüber entnehmen Sie bitte der Datei Imprints.txt in der Samba-Distribution). Ein Imprints-Treiberpaket ist, kurz gesagt, ein gzip-komprimiertes tar-Archiv mit den Treiberdateien, den relevanten INF-Dateien sowie einer Steuerdatei, die das Installationsprogramm benötigt.

17.9.3 Der Imprints-Server

Der Imprints-Server ist eigentlich ein Datenbankserver, der über standardisierte HTTP-Mechanismen abgefragt werden kann. Zu jedem Druckereintrag in der Datenbank gehört eine URL für das eigentliche Herunterladen des Pakets. Jedes Paket ist mit Hilfe von GnuPG digital signiert, so dass man überprüfen kann, ob das heruntergeladene Paket wirklich dasjenige in der Imprints-Datenbank ist. Es wird sehr empfohlen, diese Sicherheitsüberprüfung nicht zu deaktivieren.

17.9.4 Das Installationsprogramm

Weitergehende Informationen zum Imprints-Installationsprogramm finden Sie in der Dokumentationsdatei `Imprints-Client-HOWTO.ps`, die im Imprints-Quellpaket enthalten ist. Das Imprints-Installationsprogramm gibt es in zwei verschiedenen Ausführungen:

- Als eine Anzahl von Perl-Kommandozeilenskripten
- Als eine auf GTK+ basierende grafische Schnittstelle zu den Perl-Kommandozeilenskripten

Das Installationsprogramm bietet (in beiden Ausführungen) die Möglichkeit, den Imprints-Datenbankserver nach einer Namensliste passender Druckermodelle abzufragen, ebenso wie die Möglichkeit, die Treiber auf entfernten Samba- und Windows NT-Druckerservern herunterzuladen und zu installieren.

Der grundlegende Installationsvorgang besteht aus vier Schritten, und der Perl-Code ist um smbclient und **rpcclient** herum aufgebaut.

- Für jede unterstützte Architektur eines gegebenen Druckers:

1. rpcclient: Hole das passende Verzeichnis zum Hochladen auf dem entfernten Server.
2. smbclient: Lade die Treiberdateien hoch.
3. rpcclient: Setze ein AddPrinterDriver() MS-RPC ab.

- rpcclient: Setze ein AddPrinterEx() MS-RPC ab, um den Drucker tatsächlich zu erstellen.

Eines der Probleme bei der Implementierung des Imprints-Tool-Sets bestand in den Namensräumen zwischen verschiedenen unterstützten Client-Architekturen. Windows NT zum Beispiel enthält einen Treiber namens „*Apple LaserWriter II NTX v51.8*“, und Windows 95 nennt seine Version dieses Treibers „*Apple LaserWriter II NTX*“.

Das Problem besteht darin zu wissen, welche Client-Treiber für einen Drucker hochgeladen wurden Aufmerksame Leser werden sich erinnern, dass das Dialogfeld **Druckereingeschaften** in Windows NT nur Platz für den Namen eines Druckertreibers enthält. Ein schneller Blick auf die System-Registry von Windows NT 4.0

```
HKLM\System\CurrentControlSet\Control\Print\Environment
```

genügt, um festzustellen, dass Windows NT immer den NT-Treibernamen benutzt. Das ist in Ordnung, da Windows NT immer verlangt, dass mindestens die Windows NT-Version des Druckertreibers vorhanden ist. Samba verlangt das intern nicht, also: „*Wie kann man den NT-Treibernamen benutzen, falls er noch nicht installiert wurde?*“

Man umgeht diese Einschränkung dadurch, dass man verlangt, dass alle Imprints-Druckertreiberpakete sowohl für Intel Windows NT als auch für 95/98 Druckertreiber enthalten und dass der NT-Treiber als Erstes installiert wird.

17.10 Netzwerkdrucker ohne Benutzerinteraktion hinzufügen

Folgender Artikel aus der MS Knowledge-Base kann eventuell hilfreich sein, wenn Sie mit Clients unter Windows 2000 umgehen müssen: *How to Add Printers with No User Interaction in Windows 2000,* (<`http://support.microsoft.com/default.aspx?scid=kb;en-us;189105`>). Er gilt auch für Clients unter Windows XP Professional. Die in diesem Abschnitt skizzierten Ideen wurden von diesem Artikel inspiriert, der eine Methode auf der Kommandozeile beschreibt, mit der Netzwerk- und lokale Drucker und ihre Treiber installiert werden können. Am nützlichsten ist sie, wenn sie in Anmeldeskripten integriert wird. Welche Optionen verfügbar sind, können Sie sehen, wenn Sie folgenden Befehl in einer **DOS-Shell** eingeben:

```
rundll32 printui.dll,PrintUIEntry /?
```

Es erscheint ein Fenster, das Ihnen alle verfügbaren Kommandozeilenschalter anzeigt. Eine umfangreiche Beispielliste ist ebenfalls vorhanden. Das geht nur bei Windows 200x/XP, aber nicht bei Windows NT. Windows NT verfügt vermutlich über einige andere Werkzeuge im entsprechenden Resource Kit. Hier ist ein Vorschlag dafür, was ein Client-Anmeldeskript enthalten könnte, mit einer kurzen Erklärung dessen, was die Zeilen wirklich tun (es funktioniert, wenn Windows 200x/XP-Clients über Samba auf Drucker zugreifen, und für Windows-basierte Druckerserver funktioniert es auch):

```
rundll32 printui.dll,PrintUIEntry /dn /n "\\cupsserver\infotec2105-IPDS" /q
rundll32 printui.dll,PrintUIEntry /in /n "\\cupsserver\infotec2105-PS"
rundll32 printui.dll,PrintUIEntry /y /n "\\cupsserver\infotec2105-PS"
```

Dies ist eine Liste der verwendeten Kommandozeilen-Parameter:

/dn löscht einen Netzwerkdrucker.

/q stiller Modus.

/n benennt einen Drucker.

/in fügt eine Netzwerkdruckerverbindung hinzu.

/y stellt den Drucker als Standarddrucker ein.

- Zeile 1 löscht einen vorher eventuell vorhandenen Netzwerkdrucker *infotec2105-IPDS* (der native Windows-Treiber mit LPRng benutzt hatte, die vom Server entfernt wurden, als der Server auf CUPS umgestellt wurde). Das **/q** am Ende verhindert, dass Bestätigungs- oder Fehlerdialogfelder eingeblendet werden. Diese sollten bei einem Benutzer nicht erscheinen, der sich gerade anmeldet.
- Zeile 2 fügt den neuen Drucker *infotec2105-PS* hinzu (der tatsächlich das gleiche physische Gerät ist, aber nun vom neuen CUPS-Drucksystem betrieben wird und mit den CUPS/Adobe-PS-Treibern verbunden ist). Der Drucker und sein Treiber müssen in Samba hinzugefügt worden sein, bevor der Benutzer sich anmeldet (z.B. durch eine Prozedur, wie sie oben in diesem Kapitel beschrieben wurde, oder durch die Ausführung von **cupsaddsmb**). Der Treiber wird nun automatisch auf den Client-PC heruntergeladen, auf dem der Benutzer sich gerade anmeldet.
- Zeile 3 setzt den Standarddrucker auf diesen neuen Netzwerkdrucker (es mag mehrere andere auf die gleiche Art installierte Drucker geben, und einige können auch lokal sein, daher haben wir uns für einen Standarddrucker entschieden). Die Wahl des Standarddruckers darf für verschiedene Benutzer natürlich unterschiedlich sein.

Die zweite Zeile funktioniert nur, wenn der Drucker *infotec2105-PS* eine bereits funktionierende Druckerschlange auf dem `cupsserver` hat und wenn die Druckertreiber erfolgreich ins Treiber-Repository *`[print$]`* von Samba hochgeladen wurden (mit **APW**, **smbclient/rpcclient** oder **cupsaddsmb**). Manche Samba-Versionen vor der Version 3.0 verlangten nach der Druckerinstallation und dem Hochladen des Treibers einen Neustart von smbd, wenn das Skript (oder irgendein anderer Vorgang, bei dem ein Treiber heruntergeladen wurde) nicht versagen sollte.

Da es keine einfache Methode gibt, aus dem Anmeldeskript heraus zu testen, ob ein installierter Netzwerkdrucker vorhanden ist, sollten Sie es erst gar nicht versuchen, sondern

die Deinstallation/Reinstallation jedes Mal gestatten, wenn ein Benutzer sich anmeldet. Es passiert sowieso sehr schnell (in 1 bis 2 Sekunden).

Weitere Vorteile hiervon sind:

- Alle Änderungen an den Standardeinstellungen des Druckers werden automatisch bei jeder Benutzeranmeldung weitergegeben.
- Benutzer haben die gleichen Einstellungen auch bei der Anmeldung von verschiedenen Workstations in die Domäene („*roaming*“).

Da Netzwerkdrucker pro Benutzer installiert werden, erleichtert es das ungemein, die Installation immer aktuell zu halten. Die wenigen zusätzlichen Sekunden bei der Anmeldung sind kaum bemerken. Drucker können nach Belieben auf dem Server zentral hinzugefügt, verändert und gelöscht werden, ohne dass auf den Clients ein Eingriff von Benutzerseite nötig wäre (Sie müssen lediglich die Anmeldeskripten aktualisieren).

17.11 Der Befehl addprinter

Der Befehl **addprinter** kann so konfiguriert werden, dass er von Samba als Shell-Skript oder als Programm ausgeführt wird. Er wird dann aufgerufen, wenn APW von einem Client auf dem Samba-Druckerserver ausgeführt wird. Der APW bittet den Benutzer, mehrere Felder auszufüllen, z.B. Druckername, verwendeter Treiber, Kommentar, Port-Monitor usw. Diese Parameter werden vom APW an Samba weitergegeben. Falls der Befehl **addprinter** so entworfen ist, dass er einen neuen Drucker erstellen kann (dadurch, dass auf älteren Systemen korrekte printcap-Einträge geschrieben werden oder auf moderneren Systemen der Befehl **lpadmin** ausgeführt wird) und die entsprechende Freigabe erstellen kann, dann erzeugt der APW in Samba und dem UNIX-Drucksubsystem tatsächlich einen neuen Drucker!

17.12 Migration von klassischem Drucken zu Samba

Die grundlegende NT-artige Druckertreiberverwaltung hat sich in Version 3.0 nicht wesentlich gegenüber den Versionen 2.2.x verändert (abgesehen von vielen kleinen Verbesserungen). Hier sollte die Migration sehr einfach sein, besonders, wenn Sie den obigen Ratschlag befolgt haben, veraltete Parameter in Ihren Einstellungen nicht mehr zu benutzen. Mehr Aufwand ist es bei der Migrationen einer vorhandenen Einstellung unter 2.0.x oder wenn Sie in Ihren Samba 2.2-Installationen weiterhin auf die Art von Windows 9x/Me gedruckt haben. Lesen Sie bitte die entsprechenden Release Notes und die HOWTO-Collection für Samba-2.2.x. Sie können mehrere Wege einschlagen. Hier sind einige mögliche Migrationsszenarien:

- Sie müssen die neue Drucker- und Treiberunterstützung für Windows NT studieren und anwenden. Die vorher benutzten Parameter *printer driver file*, *printer driver* und *printer driver location* werden nicht mehr unterstützt.
- Wenn Sie von der Druckertreiberunterstützung in Windows NT profitieren möchten, müssen Sie auch die Windows 9x/Me-Treiber auf die neuen Einstellungen migrieren.
- Eine vorhandene Datei `printers.def` (die in dem nun entfernten Parameter *printer driver file* angegeben wird) wird in Samba-3 nicht mehr funktionieren. In 3.0 versucht smbd, Treiberdateien für Windows 9x/Me für den Drucker in *[print$]* sowie

weitere Einstellungen in der TDB zu finden, und zwar nur dort. Schlägt das fehl, weicht es *nicht* darauf aus, ein `printers.def` (und alle dazugehörigen Parameter) zu benutzen (so wie es in 2.2.x der Fall war). Das Werkzeug **make_printerdef** ist entfernt worden, und es gibt dafür nichts, was rückwärtskompatibel wäre.

- Sie müssen einen Windows 9x/Me-Treiber in die Freigabe *[print$]* für einen Drucker auf Ihrem Samba-Host installieren. Die Treiberdateien werden in dem Unterverzeichnis „*WIN40/0*“ von *[print$]* gespeichert, und einige andere Einstellungen und Informationen gehen in die druckrelevanten TDBs ein.
- Wenn Sie eine vorhandene Datei `printers.def` in die neue Einstellung migrieren möchten, besteht die einzige aktuelle Lösung darin, den APW von Windows NT für die Installation der NT- und 9x/Me-Treiber zu benutzen. Mit smbclient und rpcclient kann das auch aus Skripten heraus geschehen, wie das folgende Imprints-Installationsprogramm an einem Beispiel zeigt:

  <`http://imprints.sourceforge.net/`>

  Lesen Sie auch im Abschnitt „*Unterstützung des CUPS-Drucksystems*“ nach, wie **rpcclient** benutzt wird.

17.13 Druckerinformation in Active Directory oder LDAP veröffentlichen

Dieser Punkt wird in einer späteren Fassung dieses Dokuments behandelt. Wenn Sie gern Ihre Hilfe anbieten möchten, um das zu dokumentieren, kontaktieren Sie bitte John H. Terpstra. <`mail://jht@samba.org`>

17.14 Häufige Fehler

17.14.1 Ich gebe mein root-Passwort ein, erhalte aber keinen Zugang

Verwechseln Sie nicht das root-Passwort, das im UNIX-System gültig ist (und in den meisten Fällen in Form eines Einweg-Hashes in einer Datei namens `/etc/shadow` gespeichert ist), mit dem Passwort bei der Identifikation durch Samba. Samba kennt das UNIX-Passwort nicht. Ein root-Zugang zu Samba-Ressourcen erfordert, dass zuerst ein Samba-Konto für root erstellt wird. Dies erledigt man wie folgt mit dem Befehl **smbpasswd**:

```
root#  smbpasswd -a root
New SMB password: secret
Retype new SMB password: secret
```

17.14.2 Mein Druckauftrag gelangt ins Spooling-Verzeichnis, geht dann aber verloren

Benutzen Sie nicht das vorhandene spool-Verzeichnis des UNIX-Drucksystems als spool-Verzeichnis für Samba. Es mag bequem und platzsparend erscheinen, führt aber nur zu

Problemen. Die zwei Verzeichnisse müssen verschieden sein.

17.15 Aktualisierung

Seit Erst-Veröffentlichung dieses Buches in Englisch haben die Samba-Versionen 3.0.1 bis 3.0.7 wichtige Aktualisierungen und Änderungen erfahren. Die Entwickler beseitigten verschiedene Fehler und schlossen Sicherheitslücken. Viele Modifikationen betrafen auch die Druckfunktionen. Hier eine kurze Übersicht:

'rpcclient adddriver' akzeptiert jetzt die Angabe der Treiber-Version. Dies ermöglicht die kontrollierte Installation von 'Kernel Mode'- und 'User Mode'-Druckertreibern. (Änderung seit 3.0.1)

Beispiel:

```
root# rpcclient localhost -N   \
           -U'root%secret' \
           -c 'adddriver "Windows NT x86"  \
           "infotec_2105:cupsdrv5.dll:infotec_2105.ppd:\
           cupsui5.dll:cups5.hlp:NULL:RAW:NULL" \
           2'
```

'printing = ...' ist jetzt nicht mehr 'globaler', sondern 'service level'-Parameter. Dies erlaubt mehr Flexibilität und eine bequemere Verwirklichung eigener Druckbefehle ('print command' in `smb.conf`), unterschiedlich pro Druckerwarteschlange. (Änderung seit 3.0.3)

Beispiel:

```
printing = sysvprinting = sysv
```

'cups options = ...' erlaubt die Angabe von Druckuptionen wie z.B '-o raw' ohne in die Konfiguration des CUPS-Servers eingreifen zu müssen. (neuer Parameter seit 3.0.3)

Beispiel:

```
cups options = 'raw,media=a4,job-sheets=secret,secret'cups options = 'raw,media=a
```

'printcap cache time = ...' legt das Zeitintervall in Sekunden fest, in dem Samba die 'printcap' nach neu hinzugekommenen (oder gelöschten) Druckerwarteschlangen untersucht. (neuer Parameter seit 3.0.6)

Beispiel:

```
printcap cache time = 60printcap cache time = 60
```

'rpcclient setprintername' ermöglicht die Zuordnung eines anderen Namens zu einer Druckerwarteschlange. Dieser Name wird den Windows-Clients gezeigt (Unix-Benutzer sehen den ursprünglichen Namen). (neuer Parameter seit 3.0.6)

Beispiel:

```
root# rpcclient localhost -N   \
    -U'root%secret' \
    -c 'setprintername cups_printer "Drucker für Gruppe Marketing"'
```

'cups server = ...' erlaubt die Verwendung eines von 'localhost' unterschiedlichen CUPS-Servers. Unterschiedliche virtuellen smbd-Prozessen können sogar unterschiedliche cups server verwenden. (neuer Parameter seit 3.0.6) Beispiele:

```
cups server = 10.160.61.60cups server = 10.160.61.60
cups server = cups2.domain.comcups server = cups2.domain.com
```

'VampireDriverFunctions' ist ein neues Migrationstool seit 3.0.3 zum zeitsparenden Klonen und Transfer von Windows-Druckertreibern von einem (Windows- oder Samba-)Printserver zu einem anderen. (neu enthalten seit 3.0.3)

Nähere Erläuterungen siehe unten.

Eine ausführliche Beschreibung zu den einzelnen Punkten finden Sie am Ende des nächsten Kapitels, 'Unterstützung des CUPS-Drucksystems'.

Kapitel 18

UNTERSTÜTZUNG DES CUPS-DRUCKSYSTEMSDIE CUPS-FILTER-ARCHITEKTUR

18.1 Einleitung

18.1.1 Eigenschaften und Vorzüge

Das Common UNIX Print System (CUPS <`http://www.cups.org/`>) ist mittlerweile sehr populär geworden. Alle großen Linux-Distributionen liefern es als das Standard-Drucksystem aus. Für viele ist es ein mystisches Tool. Meistens funktioniert es einfach. Daher wird es oft als „*Black Box*“ angesehen, und solange es funktioniert, möchte sich auch niemand damit befassen. Sobald aber ein kleines Problem auftritt, bekommt man Schwierigkeiten damit herauszufinden, wie man mit der Fehlersuche beginnt. Sehr viele Informationen, die auch für CUPS relevant sind, finden Sie im Kapitel „*Klassische Druckerunterstützung*“.

CUPS bietet einige mächtige und einmalige Möglichkeiten. Neu ist auch die sehr einfache Handhabung der grundsätzlichen Funktionen. Da diese Funktionen anders sind als in den mehr traditionell orientierten Drucksystemen, wenden Sie am besten nicht Ihr bisheriges Wissen bezüglich des Druckens an. Versuchen Sie eher, CUPS von Grund auf zu verstehen. Diese Dokumentation soll dazu beitragen, dass Sie CUPS wirkllich verstehen. Beginnen wir mit den grundsätzlichen Dingen.

18.1.2 Überblick

CUPS ist mehr als nur ein System für das Printspooling. Es ist ein komplettes Drucker-Management-System, das das neue Internet Printing Protocol (IPP) erfüllt. IPP ist ein IETF-Standard (Internet Engineering Task Force) für das Drucken in Netzwerken. Viele seiner Funktionen können remote oder lokal über einen Webbrowser verwaltet werden (Bereitstellung eines plattformunabhängigen Zugriffs auf den CUPS-Printserver). Zusätzlich hat es die traditionellen Kommandozeilen-Tools und weitere moderne GUI-Schnittstellen (GUI-Schnittstellen von Drittherstellern, wie etwa das überwältigende, in KDE enthaltene KDEPrint <`http://printing.kde.org/`>).

CUPS erlaubt das Anlegen von „*raw*“- Druckern (keine Übersetzung der Druckdaten) genauso wie von „*smarten*“ Druckern (Cups übersetzt das Dateiformat in das benötigte Druckerformat). Dies gibt CUPS auf vielfache Arten ähnliche Fähigkeiten wie dem MS Windows Print Monitoring System. Falls Sie ein CUPS- Verfechter sind, dann werden Sie sicher argumentieren, dass CUPS sogar besser ist! Wie auch immer, lassen Sie uns damit weitermachen, wie man CUPS für eine Zusammenarbeit mit MS Windows-Druckclients über SAMBA konfigurieren kann.

18.2 Grundlegende Konfiguration für die CUPS-Unterstützung

In Samba-3.0 (gilt auch für 2.2.x) sind für das grundlegende Drucken mit CUPS nur zwei Einträge nötig: printing = cups und printcap = cups. CUPS benötigt keine printcap-Datei. Dennoch gibt es in der Konfigurationsdatei `cupsd.conf` zwei zugehörige Einträge, die kontrollieren, wie diese Datei anzulegen und zu verwalten ist, damit Anwendungen von Drittherstellern damit umgehen können (Beispiel: *`Printcap /etc/printcap`* und *`PrintcapFormat BSD`*). Ältere Programme benötigen oft diese printcap-Datei mit den Namen der Drucker, um drucken zu können. Stellen Sie daher sicher, dass CUPS so konfiguriert wurde, dass diese printcap-Datei erstellt und gewartet wird. Die Details finden Sie auf der Manpage **man cupsd.conf**, in den CUPS-relevanten Dokumentationen sowie in den vielen Infos vom CUPS-Server selbst: <`http://localhost:631/documentation.html`>.

18.2.1 Das Verlinken von smbd mit libcups.so

Samba hat eine spezielle Beziehung zu CUPS. Samba kann mit Unterstützung für die CUPS-Library übersetzt werden. Die meisten aktuellen Installationen haben diesen Support bereits per Default in smbd und den anderen Samba-Binaries integriert. Sie können CUPS auch benutzen, wenn Samba nicht gegen die `libcups.so` — gelinkt ist, aber es gibt einige Unterschiede in den benötigten oder unterstützten Konfigurationen.

Wenn Samba mit `libcups` kompiliert worden ist, verwendet printcap = cups die CUPS-API, um Drucker aufzufinden, Jobs zu übergeben, Queues abzufragen usw. Sonst wird dies mit der zusätzlichen **-oraw**-Option auf die System V-Druck-Kommandos umgesetzt. Auf einem Linux-System können Sie mit dem Utility **ldd** nähere Details erfahren (ldd muss nicht auf allen Plattformen vorhanden sein, seine Funktionen können auch in einem vergleichbaren Programm enthalten sein).

```
root# ldd ‘which smbd‘
libssl.so.0.9.6 => /usr/lib/libssl.so.0.9.6 (0x4002d000)
libcrypto.so.0.9.6 => /usr/lib/libcrypto.so.0.9.6 (0x4005a000)
libcups.so.2 => /usr/lib/libcups.so.2 (0x40123000)
[....]
```

Die Zeile `libcups.so.2 => /usr/lib/libcups.so.2 (0x40123000)` bedeutet, dass der CUPS-Support in Samba einkompiliert wurde. In diesem Fall und bei gesetztem printing = cups *werden anderweitige manuell gesetzte print-Kommandos in* *`smb.conf`* *ignoriert*. Bitte merken Sie sich diesen wichtigen Punkt !

TIPP

Sollte es aus irgendeinem Grund nötig sein, Ihre eigenen Druck-Kommandos zu setzen, können Sie dies erreichen, in dem Sie die Option printing = sysv verwenden. Sie verlieren so jedoch die Unterstützung der engen CUPS/Samba-Integration. Wenn Sie das vorhaben, müssen Sie folgende Druckkommandos manuell konfigurieren (am wichtigsten: print command; andere Kommandos sind lppause command, lpresume command, lpq command, lprm command, queuepause command und queue resume command).

18.2.2 Einfache smb.conf-Einstellungen für CUPS

Als Zusammenfassung zeigt das folgende Beispiel ein einfaches drucker-relevantes Setup für `smb.conf`, um den grundlegenden Support für CUPS zu erhalten:

Beispiel 18.2.1. Einfachste drucker-bezogene smb.conf

```
[global]
       load printers = yes
       printing = cups
       printcap name = cups

[printers]
       comment = Alle Drucker
       path = /var/spool/samba
       browseable = no
       public = yes
       guest ok = yes
       writable = no
       printable = yes
       printer admin = root, @ntadmins
```

Das ist alles, was Sie an grundlegenden Einstellungen zum Drucken mit CUPS benötigen. Dies wird alle Grafik-, Text-, PDF- und Postscript-Dateien drucken, die von Ihren Windows-Clients übermittelt werden. Aber die meisten Ihrer Windows-Benutzer würden nicht wissen, wie sie solche Dateien ohne einen grafischen Druckerdialog übermitteln können. Windows-Clients haben meist lokale Druckertreiber installiert, die in den Anwendungen durch den Druck-Button aktiviert werden. Ihre Benutzer drucken auch selten Dateien aus der Kommandozeile. Im Gegensatz zu Unix-Clients senden sie kaum Grafik-, Text- oder PDF- formatierte Dateien direkt zum Spooler. Sie drucken fast ausschließlich aus GUI-Anwendungen über den „*Druckertreiber*“, der zwischen der nativen Ausgabe des Programms und dem

Druckdatenstrom sitzt. Ist das Ausgabegerät kein PostScript-Drucker, so ist der Druckdatenstrom in einem „*Binärformat*“, das nur der betreffende Drucker versteht. Lesen Sie bitte weiter, um zu verstehen, welche Probleme dabei entstehen und wie Sie diese vermeiden.

18.2.3 Komplexere CUPS-Einstellungen in der smb.conf

Die nächste Konfiguration beschreibt ein etwas komplexeres Drucker-Setup der `smb.conf`. Es aktiviert generellen CUPS-Druck-Support für alle Drucker, definiert aber einen Drucker, der davon abweichend konfiguriert wird.

Beispiel 18.2.2. Das Aufheben globaler CUPS-Einstellungen für einen Drucker

```
[global]
        printing = cups
        printcap name = cups
        load printers = yes

[printers]
        comment = Alle Drucker
        path = /var/spool/samba
        public = yes
        guest ok = yes
        writable = no
        printable = yes
        printer admin = root, @ntadmins

[special_printer]
        comment = Ein spezieller Drucker mit seinen eigenen Einstellungen
        path = /var/spool/samba-special
        printing = sysv
        printcap = lpstat
        print command = echo NEW: ‘date‘: printfile %f"\
>> /tmp/smbprn.log ; \
echo „date‘: p-%p s-%s f-%f">> /tmp/smbprn.log ; \
echo „date‘: j-%j J-%J z-%z c-%c">> /tmp/smbprn.log : rm %f
        public = no
        guest ok = no
        writable = no
        printable = yes
        printer admin = kurt
        hosts deny = 0.0.0.0
        hosts allow = turbo_xp, 10.160.50.23, 10.160.51.60
```

Diese spezielle Freigabe ist nur für Testzwecke gedacht. Sie schreibt den Druckauftrag nicht in eine Datei, sondern protokolliert nur die Auftragsparameter, die Samba bekannt sind, in die Datei `/tmp/smbprn.log` und löscht die Auftragsdatei. Außerdem ist der Parameter printer admin dieser Freigabe „*kurt*“ (nicht die Gruppe „*@ntadmins*“), Gast-Zugriff ist nicht

erlaubt, die Freigabe wird nicht in der Netzwerkumgebung angezeigt (also müssen Sie wissen, dass es sie gibt), und sie erlaubt nur den Zugriff von nur drei Hosts. Um CUPS daran zu hindern, sich hier einzumischen und die Druckjobs dieser Freigabe zu übernehmen, müssen wir dies setzen: printing = sysv und printcap = lpstat.

18.3 Erweiterte Konfiguration

Bevor wir in all die Konfigurationsoptionen eintauchen, lassen Sie uns ein paar Punkte klären. *Netzwerk-Druck muss organisiert und korrekt eingerichtet werden.* Dies passiert meistens nicht. Bestehenden alten Systemen oder LAN-Umgebungen in kleinen Firmen mangelt es oft an Design und guter Wartung.

18.3.1 Zentrales Spooling vs. „*Peer-to-Peer*"-Druck

Viele kleine Büro- oder Heim-Netzwerke, genauso wie schlecht organisierte größere Umgebungen, erlauben jedem Client einen direkten Zugriff auf verfügbare Netzwerkdrucker. Dies ist im Allgemeinen eine schlechte Idee. Es blockiert oft den Zugriff eines Clients auf den Drucker, wenn der Auftrag eines anderen Clients gedruckt wird. Dies könnte die Applikation des ersten Clients ëinfrieren", während diese darauf wartet, den Auftrag loszuwerden. Es gibt auch immer wieder Beschwerden darüber, dass Aufträge gedruckt werden, deren Seiten miteinander vermischt sind. Ein besseres Konzept ist die Verwendung eines Druck-Servers; er routet alle Aufträge durch ein zentrales System, das unverzüglich antwortet, Aufträge von mehreren verschiedenen Clients zur selben Zeit annimmt und diese danach in der korrekten Reihenfolge an die Drucker weiterleitet.

18.3.2 RawPrint Serving — Hersteller-Treiber auf den Windows-Clients

Die meisten traditionell konfigurierten UNIX-Druck-Server, die für Sambas Windows-Clients arbeiten, zeigen ein wirklich simples Setup. Ihre einzige Aufgabe war die Verwaltung des „*raw spooling*" aller Jobs, die ihnen von Samba übergeben wurde. Dieser Ansatz bedeutete, dass von den Windows-Clients erwartet wurde, dass sie die Druckauftragsdatei so vorbereiten, dass diese bereit zum Versenden an das Drucker-Gerät ist. Hier muss ein nativer (vom Hersteller bereitgestellter) Windows-Druckertreiber für das Zielgerät auf jedem einzelnen Client installiert werden.

Es ist möglich, CUPS, Samba und Ihre Windows-Clients in derselben traditionellen und simplen Art zu konfigurieren. Wenn CUPS-Drucker für die Betriebsart RAW-print-through konfiguriert sind, ist es die Verantwortung des Samba-Clients, den Druckauftrag (die Datei) vollständig wiederzugeben. Die Datei muss in einem Format gesendet werden, das passend für die direkte Weitergabe an den Drucker ist. Clients müssen dafür die vom Hersteller bereitgestellten Treiber verwenden, CUPS wird keinerlei Format-Wandlung durchführen.

Die einfachste mögliche Druck-Konfiguration ist die Verwendung von raw print-through". Dies wird dadurch erreicht, dass der Drucker so installiert wird, als ob er physisch an den Windows-Client angeschlossen wäre. Sie leiten dann die Ausgabe auf eine raw-Netzwerk-Druck-Warteschlange um. Dazu ist folgendes Vorgehen erforderlich:

1. Editieren Sie `/etc/cups/mime.types`, um die Zeile nahe dem Dateiende auszukommentieren, die dies enthält:

   ```
   #application/octet-...
   ```

2. Machen Sie dasselbe mit der Datei `/etc/cups/mime.convs`.
3. Fügen Sie über das Web-Interface einen raw-Drucker hinzu. Gehen Sie mit Ihrem Browser auf `http://localhost:631`. Klicken Sie auf **Administration**, und fügen Sie den Drucker gemäß der Aufforderungen hinzu. Installieren Sie keine Treiber dafür. Wählen Sie „*Raw*“. Wählen Sie den Queue-Namen `Raw Queue`.
4. Im Abschnitt `[printers]` der Datei `smb.conf` fügen Sie Folgendes hinzu: use client driver = Yes. Im Abschnitt `[global]` schreiben Sie: printing = CUPS und printcap = CUPS.
5. Installieren Sie den Drucker, als ob er ein lokaler Drucker wäre, z.B.: Drucken auf `LPT1:`.
6. Editieren Sie die Konfiguration im Tab **Detail**, und legen Sie einen `local port` an, der auf die raw-Druck-Queue zeigt, die Sie oben angelegt haben. Beispiel: `\\server\raw_q`. Hier ist `raw_q` der Name, den Sie der Drucker-Warteschlange in der CUPS-Umgebung gegeben haben.

18.3.3 Installation von Windows-Client-Treibern

Die Druckertreiber auf den Windows-Clients können auf zwei funktional verschiedene Arten installiert werden:

- Sie installieren die Treiber manuell, und zwar einen nach dem anderen lokal auf jedem Client; dies sorgt für ein Drucken im alten *LanMan*-Stil und verwendet eine Verbindung vom Typ `\\sambaserver\druckerfreigabe`.
- Ablegen und Vorbereiten der Treiber (für den späteren Download) auf dem Druckserver (Samba); dies befähigt die Clients, „*Point'n'Print*“ zu verwenden, um Treiber semi-automatisch installiert zu bekommen, wenn sie das erste Mal auf den Drucker zugreifen; bei dieser Methode verwenden NT/200x/XP-Clients Druckaufrufe vom Typ *SPOOLSS/MS-RPC*.

Wir empfehlen, die zweite Methode zu verwenden.

18.3.4 Explizites Aktivieren von „*raw*“-Druck für *application/octet-stream*

Wenn Sie die erste Variante verwenden (Treiber werden auf Client-Seite installiert), gibt es eine Einstellung, die Sie beachten müssen: CUPS muss mitgeteilt werden, dass es den „*raw*“-Druck von Binär-Dateiformaten erlauben soll. Die CUPS-Dateien, die korrekt für RAW-Modus-Drucker gesetzt sein müssen, sind:

- `/etc/cups/mime.types`
- `/etc/cups/mime.convs`

Beide enthalten Einträge (am Ende der jeweiligen Datei), die auskommentiert werden müssen, um den RAW-Modus-Betrieb zu erlauben. In `/etc/cups/mime.types` muss folgende Zeile vorhanden sein:

```
application/octet-stream
```

In `/etc/cups/mime.convs` müssen Sie diese Zeile haben:

```
application/octet-stream   application/vnd.cups-raw   0   -
```

Wenn diese beiden Dateien nicht korrekt für RAW-Windows-Client-Druck konfiguriert sind, kann es sein, dass Sie die gefürchtete Meldung `Unable to convert file 0` in Ihrer CUPS-error_log-Datei vorfinden.

ANMERKUNG

Das Editieren von `mime.convs` und `mime.types` *erwingt* den „*raw*"-Druck nicht, es *erlaubt* ihn nur.

Hintergrund. Da CUPS ein sicherheitsbewussteres Drucksystem ist als die traditionellen Systeme, erlaubt es in der Voreinstellung nicht, dass ein Benutzer beliebige (möglicherweise binäre) Daten an Druckgeräte sendet. Dies könnte leicht dazu benutzt werden, einen „*Denial of Service*"-Angriff auf Ihre(n) Drucker zu starten, was zumindest den Verlust von einer Menge Papier und Tinte nach sich ziehen würde. „*Unbekannte*" Daten werden von CUPS als *`MIME type: application/octet-stream`* gekennzeichnet, und es wird ihnen nicht erlaubt, zum Drucker zu gelangen. In der Voreinstellung können Sie nur andere (bekannte) MIME-Typen „*raw*" senden. Das „*raw*"-Senden von Daten bedeutet, dass CUPS nicht versucht, die Daten zu konvertieren und sie einfach unangetastet an den Drucker weiterleitet (im nächsten Kapitel finden Sie noch mehr Hintergrund-Erklärungen dazu).

Dies ist alles, was Sie darüber wissen müssen, um die CUPS/Samba-Combo zum „*raw*"-Drucken von Daten zu bewegen, die von Windows-Clients vorbereitet wurden, deren Herstellertreiber lokal installiert worden sind. Wenn Sie nicht an Hintergrund-Informationen zu erweitertem CUPS/Samba-Drucken interessiert sind, überspringen Sie einfach die restlichen Abschnitte dieses Kapitels.

18.3.5 Die Methoden, um Treiber auf den Server zu laden

Dieser Abschnitt beschreibt drei übliche Methoden, zuzüglich einer neuen, mit denen Druckertreiber auf den Server geladen werden können (Üpload").

Wenn Sie im MS-RPC-Stil drucken wollen, müssen Sie die Treiber zuerst auf den Samba-Server hochladen (Freigabe *`[print$]`*). Im vorangegangenen Kapitel dieser HOWTO-

Sammlung wurde bereits beschrieben, wie man Druckertreiber auf dem Samba-Host ablegt (damit die Windows-Clients diese via „*Point'n'Print*“ herunterladen und verwenden können. Dort finden Sie Beschreibungen und Referenzen zu drei Methoden, um Druckertreiber auf dem Samba-Server vorzubereiten:

- Die GUI-Methode: Upload von einem Windows-Client mit dem „*Druckerinstallations-Assistent*“
- Die Befehlszeilen-Methode: Upload von einer UNIX-Workstation mit „*smbclient/rpcclient*“
- Die Imprints-Toolset-Methode

Diese drei Methoden können genauso auf CUPS angewendet werden. Ein neuer und praktischerer Weg, um Windows-Treiber in Samba zu laden, steht zur Verfügung, wenn Sie CUPS verwenden:

- Das Werkzeug *cupsaddsmb*

cupsaddsmb wird weiter unten im Detail behandelt. Zuerst erkunden wir aber das CUPS-Filter-System und vergleichen die Windows- und UNIX-Druck-Architektur.

18.4 Erweitertes intelligentes Drucken durch Download von Postscript-Treibern

Wir wissen nun, wie man einen „*dump*“-Druckserver aufsetzt: Das ist ein Server, der Druckaufträge „*raw*“ verwaltet, also die Druckdaten unberührt lässt.

Möglicherweise müssen Sie CUPS auf eine intelligentere Art installieren. Die Gründe können mannigfaltig sein:

- Vielleicht will Ihr Chef monatliche Statistiken: Welcher Drucker hat wie viele Seiten gedruckt? Was war die durchschnittliche Größe eines Druckauftrags? Wie viele Druckaufträge gab es im Durchschnitt pro Tag? Welche Abteilung druckt wie viel?
- Vielleicht sollen Sie ein Druck-Quota-System aufbauen: Benutzer sollten nicht mehr drucken können als ein vorgeschriebenes Limit pro Periode.
- Vielleicht ist Ihr Netzwerkdruck-Setup ein komplettes Durcheinander und muss von Grund auf reorganisiert werden.
- Vielleicht haben Sie bereits zu viele „*blue screens*“ gesehen, die von Druckertreibern herrühren, die unvollständig "debuggt"wurden und im NT-„*Kernel-Modus*“ laufen?

Diese Ziele können nicht mit einem RAW-Druckserver erreicht werden. Um einen Server aufzubauen, der diesen Anforderungen entspricht, müssen Sie zuerst lernen, wie CUPS arbeitet und wie Sie seine Features aktivieren.

Was nun folgt, ist der Vergleich von einigen fundamentalen Konzepten des Windows- und UNIX-Drucks; danach folgt eine Beschreibung des CUPS-Filter-Systems: wie es arbeitet und wie Sie es beeinflussen können.

18.4.1 GDI unter Windows – PostScript auf UNIX

Netzwerkdurck ist eine der kompliziertesten und fehlerträchtigsten Alltagsaufgaben, die ein Benutzer oder Administrator zu bewältigen hat. Dies gilt für alle Betriebssysteme. Und hier sind die Gründe dafür:

Bei den meisten Dateiformaten können Sie nicht erwarten, dass die Datei einfach dadurch gedruckt wird, dass Sie sie an den Drucker schicken. Es muss eine Wandlung des Dateiformats stattfinden. Das Problem dabei ist, dass es keinen gemeinsamen Standard für Druck-Datei-Formate gibt, der für alle Hersteller und Druckertypen gelten würde. Während sich PostScript (Handelsmarke von Adobe) und - zu einem gewissen Teil - PCL (Handelsmarke von HP) dadurch zu halb offiziellen „*Standards*“ entwickelt haben, dass sie die am weitesten verbreiteten PDLs (Page Description Languages) sind, gibt es nach wie vor viele Hersteller, die „*ihr eigenes Süppchen kochen*“. (Der Grund dafür können inakzeptabel hohe Lizenzgebühren für drucker-interne PostScript-Interpreter sein usw.)

18.4.2 Windows-Treiber, GDI und EMF

Im Betriebssystem Windows wird die Formatwandlung von den Druckertreibern erledigt. Auf der Windows-Plattform haben alle Anwendungsprogrammierer eine eingebaute API zur Verfügung, das Graphical Device Interface (GDI). Es ist ein Teil und Paket des Betriebssystems selbst, um darauf aufzubauen. Dieser GDI-Kern wird als gemeinsame einheitliche Grundlage für alle Windows-Programme verwendet, um Bilder, Schriften und Dokumente *am Bildschirm (ön screen")* darzustellen, genauso wie *auf Papier (ön paper")* (Druck). Daher können Druckertreiber-Hersteller bei ihrem Druckertreiber-Input von einem wohldefinierten GDI-Output ausgehen. Das Erreichen von WYSIWYG („*What You See Is What You Get*“) ist relativ einfach, weil die On-screen-Grafik-Primitive genauso wie die on-paper gezeichneten Objekte von einer gemeinsamen Quelle stammen. Diese Quelle, die GDI, erzeugt oft ein Dateiformat namens Enhanced MetaFile (EMF). EMF wird vom Druckertreiber verarbeitet und in ein drucker-spezifisches Format konvertiert.

ANMERKUNG

Zusätzlich zur GDI-Basis in MS Windows hat Apple sich entschieden, die Papier- und Bildschirmausgaben für seine (auf BSD-UNIX basierende, wussten Sie das?) Betriebssysteme Mac OS X und Darwin auf eine gemeinsame Basis zu stellen. Apples *Core Graphic Engine* verwendet eine Abwandlung von *PDF* für alle Anzeigen.

18.4.3 UNIX Druckdatei-Konvertierung und GUI-Grundlagen

In UNIX und Linux gibt es keine vergleichbare Schicht im OS-Kernel oder dem X-Server (Bildschirm-Darstellungsserver). Jede Anwendung ist für sich selbst verantwortlich, um ihre Druckausgabe zu erzeugen. Zum Glück verwenden die meisten Postscript, und das gibt

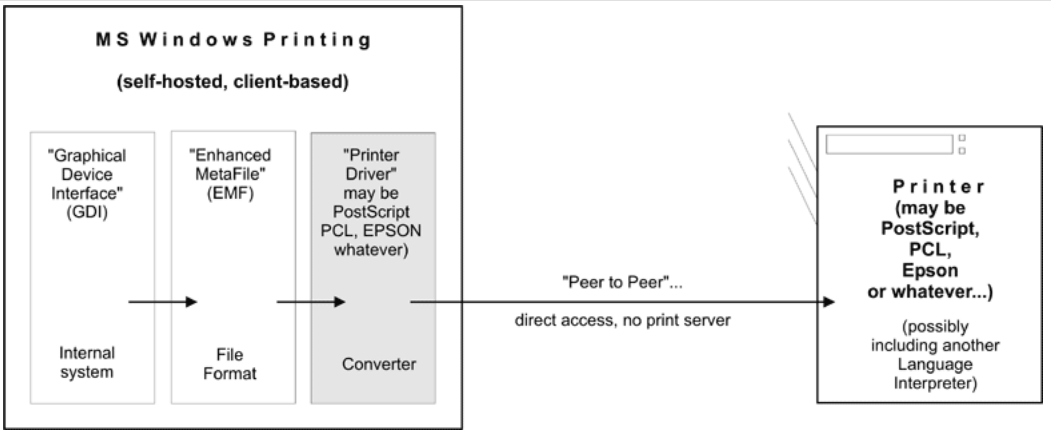


Figure 18.1. Windows druckt auf einen lokalen Drucker.

zumindest etwas gemeinsame Grundlagen. Leider gibt es viele verschiedene Qualitätsstufen für Postscript. Und, was noch schlimmer ist, es gibt einen riesigen Unterschied (und keinen gemeinsamen Ursprung) zwischen der Darstellung desselben Dokuments auf dem Bildschirm und dem Zustand, wie dieses Dokument auf Papier dargestellt wird. WYSIWYG ist schwieriger zu erreichen. Dies stammt aus der Zeit, als vor Jahrezehnten die Vorläufer von X.org beim Entwurf der UNIX-Grundlagen und -Protokolle für GUIs die Verantwortung für die „*Papierausgabe*“ ablehnten und sich auf „*nur on-screen*“ beschränkten. (Seit einigen Jahren ist das Projekt „*Xprint*“ in Entwicklung. Man versucht, Druckunterstützung in das X-Framework zu integrieren, inklusive eines PostScript- und eines PCL-Treibers, aber dieses Projekt ist noch nicht praxistauglich.) Sie können dieses unangenehme Erbe bis heute sehen, wenn Sie sich die verschiedenen „*font*“-Verzeichnisse auf Ihrem System ansehen; es gibt eigene Schriften für X-Darstellung und andere für den Druck auf Papier.

Hintergrund. Die Programmiersprache PostScript ist eine „*Erfindung*“ von Adobe Inc., aber ihre Spezifikationen wurden vollständig veröffentlicht. Ihre Stärke liegt in den mächtigen Fähigkeiten, grafische Objekte zu beschreiben (Schriften, Formen, Muster, Linien, Kurven, und Punkte), deren Attribute (Farbe, Strichstärke) und die Art, diese zu manipulieren (Skalieren, Verzerren, Rotieren, Verschieben). Wegen der offenen Spezifikation kann jeder mit entsprechenden Fähigkeiten damit beginnen, seine eigene Implementation eines PostScript-Interpreters zu schreiben und diesen zu verwenden, um PostScript-Dateien auf dem Bildschirm oder auf Papier darzustellen. Die meisten grafischen Ausgabegeräte basieren auf dem Konzept von „*Raster-Bildern*“ oder „*Pixeln*“ (eine zu erwähnende Ausnahme bilden Stift-Plotter). Natürlich können Sie eine PostScript-Datei in seiner Text-Form betrachten und ihren PostScript-Code lesen, also die Sprachbefehle, die von einem Rasterizer interpretiert werden müssen. Rasterizer erzeugen Pixel-Bilder, die von einem Viewer auf dem Schirm dargestellt werden können oder eben von einem Drucker auf dem Papier.

18.4.4 PostScript und Ghostscript

Also fehlt UNIX eine gemeinsame Basis für den Druck und die Bildschirmdarstellung. Trotz dieses ungünstigen Erbes ist das Drucken grundsätzlich ziemlich einfach, wenn Sie

PostScript-Drucker zur Verfügung haben. Der Grund dafür ist, dass diese Drucker einen eingebauten PostScript-„*Interpreter*“ besitzen, der auch Raster Image Processor (RIP) genannt wird. (Dadurch sind diese Drucker teurer als andere Drucker). Wenn Sie diesen Druckern PostScript-Daten schicken, werden diese sie auch drucken. Ihr RIP erledigt all die harte Arbeit des Umwandelns von PostScript-Zeichenbefehlen in ein Bitmap-Bild, wie Sie es auf Papier sehen, in einer Auflösung, wie Sie von Ihrem Drucker unterstützt wird. Dies entspricht dem PostScript-Druck einer Datei aus Windows.

ANMERKUNG

Traditionelle UNIX-Programme und -Druck-Systeme sind — bei Verwendung von PostScript — nicht PPD-fähig. PPDs sind „*PostScript Printer Description*“-Dateien. Sie ermöglichen es Ihnen, alle Optionen, die ein Drucker kennt, anzugeben und zu kontrollieren: Duplexdruck, Stapeln und Lochen. Daher konnten UNIX-Anwender lange Zeit viele der unterstützten Geräte- und Auftragsoptionen nicht nutzen, im Unterschied zu Windows- und Apple-Anwendern. Aber jetzt gibt es CUPS.

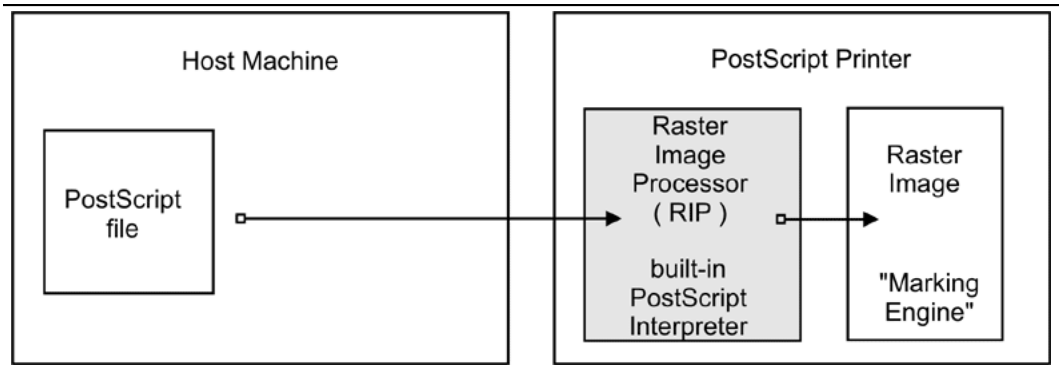


Figure 18.2. Drucken auf einen PostScript-Drucker

Jedoch gibt es auch andere Drucker-Typen da draußen. Diese Typen wissen nicht, wie man PostScript druckt. Sie verwenden ihre eigene Page Description Language (PDL, oft proprietär). Das Drucken auf diesen Geräten stellt höhere Anforderungen. Da Ihre UNIX-Anwendungen meistens PostScript erzeugen und da diese Geräte kein PostScript verstehen, müssen Sie die Druckdateien auf dem Host in ein für Ihren Drucker passendes Format konvertieren, bevor Sie diese an den Drucker senden können.

18.4.5 Ghostscript — der Software-RIP für nicht-PostScript-fähige Drucker

Hier betritt Ghostscript die Bühne. Ghostscript ist der traditionelle (und ziemlich mächtige) PostScript-Interpreter, der auf UNIX-Plattformen verwendet wird. Es ist ein RIP als Software, imstande, *viele* Datei-Konvertierungen für ein sehr großes Spektrum von Hardware-Geräten bzw. Software-Dateiformaten durchzuführen. Die Ghostscript-Technologie und -Treiber ermöglichen den PostScript-Druck auf nicht-PostScript-fähige Hardware.

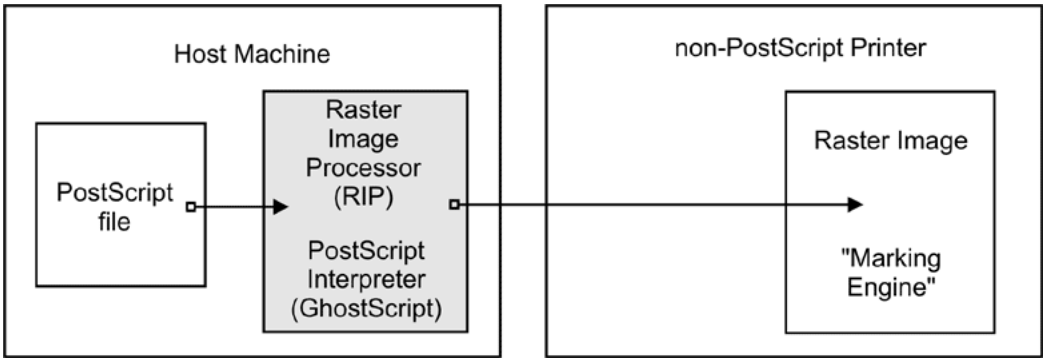


Figure 18.3. Ghostscript als RIP für nicht-PostScript-fähige Drucker

TIPP

Verwenden Sie den Befehl „*gs -h*“, um alle eingebauten „*devices*“ Ihrer Ghostscript-Version anzusehen. Wenn Sie den Parameter *-sDEVICE=png256* auf Ihrer Ghostscript-Befehlszeile angeben, teilen Sie Ghostscript mit, den Input in eine PNG-Datei zu konvertieren. Ein „*device*“ auf der Befehlszeile anzugeben ist der wichtigste Parameter, um Ghostscript exakt mitzuteilen, wie es den Input darstellen soll. Neue Versionen von Ghostscript werden in ziemlich regelmäßigen Intervallen veröffentlicht, mittlerweile von artofcode LLC. Diese Versionen werden ursprünglich unter die Lizenz „*AFPL*“ gestellt, aber dann unter der GNU GPL wiederveröffentlicht, sobald die nächste AFPL-Version erscheint. GNU Ghostscript ist wahrscheinlich die auf den meisten Samba-Systemen installierte Version. Aber es hat einige Mängel. Daher wurde ESP Ghostscript als eine Erweiterung zu GNU Ghostscript entwickelt, mit vielen Bug-fixes, zusätzlichen Geräten und Erweiterungen. Es wird gemeinsam von Entwicklern von CUPS, Gimp-Print, MandrakeSoft, SuSE, Red Hat und Debian verwaltet und entwickelt. Es beinhaltet das Gerät „*cups*“ (das essenziell wichtig ist, um von CUPS aus auf Nicht-PS-Drucker zu drucken).

18.4.6 Spezifikation der PostScript Printer Description (PPD)

Während PostScript im Kern eine Seitenbeschreibungssprache (PDL) ist, um das Layout einer Seite auf eine geräte-unabhängige Art darzustellen, werden in der Praxis Druckaufträge letztendlich immer von Hardware mit geräteabhängigen Eigenschaften ausgegeben. Um all die Unterschiede in der Hardware zu berücksichtigen und Innovation zu ermöglichen, hat Adobe eine Syntax und ein Dateiformat für PostScript-Printer-Description-(PPD-)Dateien bestimmt. Jeder PostScript-Drucker wird mit einer dieser Dateien geliefert.

PPDs enthalten all die Informationen über generelle und spezifische Eigenschaften des jeweiligen Drucker-Modells: Welche verschiedenen Auflösungen kann es verarbeiten? Hat es eine Duplex-Einheit? Wie viele Papierschächte gibt es? Welche Arten von Medien und deren Formate kann es verarbeiten? Für jeden Punkt benennen PPDs auch die spezielle Befehlsfolge, die man an den Drucker (meist innerhalb der PostScript-Datei) senden muss, um ihn zu aktivieren.

Die Information in diesen PPDs ist dafür bestimmt, von den Druckertreibern berücksichtigt zu werden. Daher wird als Teil des für einen bestimmten Drucker installierten Windows-PostScript-Treibers die PPD des Druckers installiert. Wo es Sinn macht, werden die PPD-Features in den UI-Dialogen des Treibers dargestellt, um dem Benutzer eine Auswahl von Druck-Optionen zu geben. Abschließend wird die Auswahl des Benutzers in die vom Drucker erstellte PostScript-Datei geschrieben (in der Form spezieller PostScript-, PJL-, JCL- oder herstellerspezifischer Befehle).

WARNUNG

Eine PostScript-Datei, die angelegt wurde, um gerätespezifische Befehle zum Erreichen einer bestimmten Druckausgabe (z.B. Duplexdruck, Stapeldruck oder Faltungen) auf einem bestimmten Ausgabegerät zu enthalten, kann möglicherweise nicht so drucken, wie erwartet, oder kann auf anderen Druckermodellen gar nicht zu drucken sein; es kann auch sein, dass diese Datei nicht mehr für eine weitere Verarbeitung durch Software geeignet ist (z.B. durch ein PDF-distilling-Programm).

18.4.7 Verwendung von Windows-formatierten Hersteller-PPDs

CUPS kann mit allen spezifikationsgemäßen PPDs ungehen, wie sie von Herstellern für ihre PostScript-Modelle bereitgestellt werden. Sogar wenn ein Hersteller unser Lieblingsbetriebssystem nicht in seinen Handbüchern und Broschüren erwähnt hat, können Sie sich sicher darauf verlassen: *Wenn Sie die Windows NT-Version der PPD erhalten, können Sie diese unverändert mit CUPS verwenden* und daher die volle Leistungsfähigkeit Ihres Druckers nutzen, genauso wie ein Windows NT-Benutzer es könnte!

TIPP

Um online zu prüfen, ob eine beliebige PPD der Spezifikation entspricht, gehen Sie auf <http://www.cups.org/testppd.php> und laden Ihre PPD. Sie sehen das Ergebnis sofort. CUPS hat seit der Version 1.1.19 ein weitaus strikteres internes PPD-Parsing und eine Code-Prüfung aktiviert; im Fall von Druckerproblemen sollte diese Online-Ressource eine Ihrer ersten Anlaufstellen sein.

WARNUNG

Für tatsächliche PostScript-Drucker verwenden Sie *nicht* die *Foomatic* oder *cupsomatic* PPDs von Linuxprinting.org. Mit diesen Geräten sind immer die vom Hersteller bereitgestellten PPDs die erste Wahl!

TIPP

Wenn Sie nach einer Original-Hersteller-PPD eines spezifischen Geräts suchen und Sie wissen, dass eine NT4-Maschine (oder irgendeine andere Windows-Maschine) in Ihrem LAN den PostScript-Treiber installiert hat, verwenden Sie einfach **smbclient //NT4-box/print\$ -U username**, um auf das Windows-Verzeichnis zuzugreifen, in dem alle Druckertreiber-Dateien gespeichert sind. Durchsuchen Sie zuerst das Unterverzeichnis `W32X86/2` nach den gesuchten PPDs.

18.4.8 CUPS verwendet auch PPDs für Nicht-PostScript-Drucker

CUPS verwendet auch spezielle PPDs, um mit Nicht-PostScript-Druckern umzugehen. Diese PPDs sind üblicherweise nicht von den Herstellern verfügbar (und, nein, Sie können nicht einfach die PPD eines PostScript-Druckers mit demselben Modellnamen verwenden und hoffen, dass diese auch mit der Nicht-PostScript-Version funktioniert). Um zu verstehen, wie diese PPDs funktionieren, müssen wir zuerst tief in die Architektur der CUPS-Filter und -Dateiumwandlung eintauchen. Bleiben Sie dran.

Der Kern des CUPS-Filter-Systems beruht auf Ghostscript. Zusätzlich dazu verwendet CUPS einige andere eigene Filter. Sie (oder der Hersteller Ihres Betriebssystems) können sogar noch mehr Filter hinzugefügt haben. CUPS behandelt alle Dateiformate unter der Zuordnung verschiedener MIME-Typen. Jede eintreffende Druckdatei wird einem initialen

Auto-Typing zugeführt. Dieses Auto-Typing bestimmt den MIME-Typ der Druckdatei. Ein bestimmter MIME-Typ bedingt keine oder mehrere mögliche Filter-Ketten, die für den gewählten Zieldrucker relevant sind. Dieser Abschnitt behandelt, wie die Erkennungs- und Umwandlungsregeln von MIME-Typen zusammenarbeiten. Sie werden von CUPS dazu verwendet, um automatisch eine funktionierende Filterkette für jedes beliebige Eingabe-Datenformat zu bilden.

Wenn CUPS eine PostScript-Datei in ein Bitmap rastert, passiert dies in zwei Stufen:

- Die erste Stufe verwendet ein Ghostscript-Device namens „*cups*“ (dies seit Version 1.1.15) und erzeugt ein generisches Raster-Format namens „*CUPS raster*“.
- Die zweite Stufe verwendet einen „*raster driver*“, der das generische „*CUPS raster*“ in ein gerätespezifisches Raster konvertiert.

Stellen Sie sicher, dass Ihre Ghostscript-Version das Gerät „*cups*“ einkompiliert hat (überprüfen Sie das mit **gs -h | grep cups**). Ansonsten könnten Sie das gefürchtete `Unable to convert file 0` in Ihrer CUPS-error_log-Datei vorfinden. Um „*cups*“ als Gerät in Ihrem Ghostscript zu haben, müssen Sie entweder GNU Ghostscript patchen und neu kompilieren, oder Sie verwenden ESP Ghostscript <`http://www.cups.org/ghostscript.php`>. Die bessere Alternative ist ESP Ghostscript. Es unterstützt nicht nur CUPS, sondern auch 300 andere Geräte (während GNU Ghostscript nur ungefähr 180 Geräte unterstützt). Wegen dieser breiten Unterstützung von Ausgabegeräten ist ESP Ghostscript auch die erste Wahl für Nicht-CUPS-Spooler. Es wird mittlerweile von Linuxprinting.org für alle Spooler empfohlen.

CUPS-Drucker können so eingerichtet werden, dass sie externe Darstellungspfade verwenden. Einer der gängigsten ist das Konzept Foomatic/cupsomatic von Linuxprinting.org. <`http://www.linuxprinting.org/`> Dieses verwendet den klassischen Ghostscript-Ansatz, alles auf einmal zu tun. Es verwendet nicht das Gerät „*cups*“, sondern eines der vielen anderen. Jedoch erzielt man auch bei der Verwendung von Foomatic/cupsomatic das beste Ergebnis und die breiteste Drucker-Modell-Unterstützung mit ESP Ghostscript (mehr zu cupsomatic/Foomatic, im Speziellen zur neuen Version, die jetzt *foomatic-rip* heißt, finden Sie weiter unten).

18.4.9 MIME-Typen und CUPS-Filter

CUPS liest die Datei `/etc/cups/mime.types` (und alle anderen Dateien mit einem Suffix `*.types` im selben Verzeichnis) beim Start. Diese Dateien enthalten die Regeln zur Erkennung des MIME-Typs, die angewendet werden, wenn CUPS seine Auto-Typing-Routinen ausführt. Die Regel-Syntax wird in der Manpage von `mime.types` erklärt sowie im Abschnitt commentsïn der Datei `mime.types` selbst. Eine einfache Regel sieht so aus:

```
application/pdf          pdf string(0,%PDF)
```

Das bedeutet: Wenn ein Dateiname das Suffix `.pdf` hat oder der magische String *%PDF* exakt am Beginn der Datei selbst (Offset 0 vom Start) steht, ist dies eine PDF-Datei (*application/pdf*). Eine weitere Regel ist:

```
application/postscript  ai eps ps string(0,%!) string(0,<04>%!)
```

Wenn der Dateiname eines der Suffixe `.ai`, `.eps`, `.ps` hat oder die Datei selbst mit einem der Strings *%!* oder *<04>%!* beginnt, ist es eine generische PostScript-Datei (*application/postscript*).

Warnung

Verwechseln Sie nicht die anderen mime.types-Dateien, die Ihr System verwendet, mit denen im Verzeichnis `/etc/cups/`.

Anmerkung

Es gibt einen wichtigen Unterschied zwischen zwei ähnlichen MIME-Typen in CUPS: Einer ist *application/postscript*, der andere ist *application/vnd.cups-postscript*. Während *application/postscript* geräte-unabhängig sein soll (Auftragsoptionen sind immer noch außerhalb des PS-Datei-Inhalts, von CUPS in der Befehlszeile oder Umgebungsvariablen eingebettet), kann *application/vnd.cups-postscript* die Auftragsoptionen in die Postscript-Daten selbst eingefügt erhalten (wo sich das anwenden lässt). Die Transformation des generischen PostScript-Formats (*application/postscript*) in gerätespezifisches PostScript (*application/vnd.cups-postscript*) ist die Aufgabe des CUPS-Filters *pstops*. pstops verwendet Informationen aus dem PPD, um die Transformation durchzuführen.

CUPS kann mit seinen Filtern folgende Formate und ihre zugehörigen MIME-Typen handhaben: ASCII text, HP-GL, PDF, PostScript, DVI und viele Bild-Formate (GIF, PNG, TIFF, JPEG, Photo-CD, SUN-Raster, PNM, PBM, SGI-RGB und noch mehr).

18.4.10 MIME-Typ-Umwandlungsregeln

CUPS liest die Datei `/etc/cups/mime.convs` (und alle anderen Dateien mit der Endung `*.convs` im selben Verzeichnis) beim Starten. Diese Dateien enthalten Zeilen, die einen Eingabe-MIME-Typus, einen Ausgabe-MIME-Typus, einen Format-Wandlungsfilter, der den Ausgabe-Typus aus dem Eingabe-Typus erzeugen kann, sowie virtuelle Kosten angeben, die mit dieser Umwandlung verbunden sind. Ein Beispiel für eine solche Zeile ist Folgendes:

```
application/pdf          application/postscript   33   pdftops
```

Das bedeutet, dass der Filter *pdftops* den Typ *application/pdf* als Eingabe verwenden und daraus *application/postscript* als Ausgabe erzeugen wird; die virtuellen Kosten dieser Operation sind 33 CUPS-$. Der nächste Filter ist teurer, er kostet 66 CUPS-$:

```
application/vnd.hp-HPGL application/postscript   66   hpgltops
```

Dies ist der Filter *hpgltops*, der HP-GL-Plotter-Dateien in PostScript umwandelt.

```
application/octet-stream
```

Hier zwei weitere Beispiele:

```
application/x-shell      application/postscript   33    texttops
text/plain               application/postscript   33    texttops
```

Die letzten beiden Beispiele lassen den Filter *texttops* sowohl an *text/plain* als auch an *application/x-shell* arbeiten. (Hinweis: Diese Unterscheidung wird für das Syntax-Highlighting von *texttops* benötigt).

18.4.11 Überblick über das Filtern

Es gibt viel mehr Kombinationen in `mime.convs`. Sie sind jedoch nicht darauf beschränkt, die hier vordefinierten Kombinationen zu verwenden. Sie können jeden Filter, den Sie wollen, in das CUPS-Grundgerüst einsetzen. Es muss einigen minimalen Anforderungen entsprechen oder dazu gebracht werden, ihnen zu entsprechen. Wenn Sie irgendeinen coolen Filter finden (oder schreiben), stellen Sie sicher, dass er dem entspricht, was CUPS braucht, und dass Sie die richtigen Zeilen in die Dateien `mime.types` und `mime.convs` einfügen. Dann wird er prolemlos innerhalb von CUPS arbeiten.

18.4.11.1 Anforderungen an Filter

Die erwähnten „*CUPS-Anforderungen*“ für Filter sind simpel. Nehmen Sie den Dateinamen oder `stdin` als Input, und schreiben Sie diesen auf `stdout`. Die Filter sollten die folgenden fünf bis sechs Argumente verstehen: *printer job user title copies options [filename].*

printer Der Name der Drucker-Queue (Normalerweise ist dies der Name des ausgeführten Filters.)

job Die numerische Auftrags-ID des gerade gedruckten Auftrags

user Der String aus dem Attribut originating-user-name

title Der String aus dem Attribut job-name

copies Der numerische Wert des Attributs number-copies

options Die Auftragsoptionen

filename (optional) Die Datei der Druckanfrage (wenn diese Angabe fehlt, erwarten die Filter, die Daten über `stdin` geliefert zu bekommen). In den meisten Fällen ist es einfach, ein einfaches Wrapper-Skript um Filter zu schreiben, um sie mit CUPS arbeiten zu lassen.

18.4.12 Vorfilter (Prefilters")

Wie zuvor bemerkt, ist PostScript das zentrale Dateiformat für jedes UNIX-basierende Drucksystem. Von PostScript aus generiert CUPS Rasterdaten zur Lieferung an Nicht-PostScript-Drucker.

Aber was passiert, wenn Sie eines der unterstützten Nicht-PS-Formate in den Druck schicken? Dann verwendet CUPS „*pre-filters*" auf diese Eingabeformate, um als Erstes PostScript zu erzeugen. Es gibt solche Vorfilter, um PS aus ASCII text, PDF, DVI oder HP-GL zu erzeugen. Die Ausgabe dieser Filter ist immer vom MIME Typ *application/postscript* (das bedeutet, dass jegliche geräte-spezifische Druckoptionen noch nicht von CUPS ins PS eingebettet werden, und dass der nächste aufzurufende Filter pstops ist). Ein weiterer Vorfilter läuft über alle unterstützten Bildformate, der Filter *imagetops*. Seine Ausgabe ist immer vom MIME-Typ *application/vnd.cups-postscript* (nicht application/postscript), was bedeutet, dass die Druckoptionen bereits in die Datei eingebettet sind.

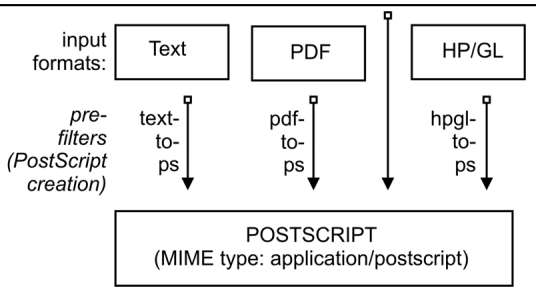


Figure 18.4. Das Vorfiltern in CUPS, um PostScript zu erzeugen

18.4.13 pstops

pstops ist der Filter, um *application/postscript* in

application/vnd.cups-postscript umzuwandeln. Es wurde bereits oben erwähnt, dass dieser Filter alle gerätespezifischen Druckoptionen (Befehle an den Drucker, um Duplexdruck, Stapeln und Lochen zu veranlassen usw.) in die PostScript-Datei einbindet.

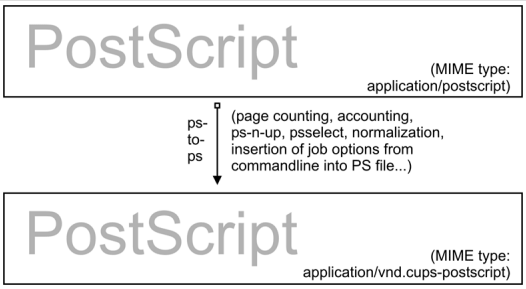


Figure 18.5. Das Hinzufügen von gerätespezifischen Druckoptionen

Das ist nicht alles. Andere ausgeführte Aufgaben sind:

- Die Auswahl der zu druckenden Seiten (wenn Sie nur die Seiten „*3, 6, 8-11, 16, 19-21*“ drucken wollen oder nur die ungeraden Seiten).
- Zwei oder mehr logische Seiten auf ein Blatt Papier drucken (die so genannte „*number-up*“-Funktion).
- Das Zählen der Seiten des Auftrags, um die Abrechnungsinformation in die Datei `/var/log/cups/page_log` zu schreiben.

18.4.14 pstoraster

pstoraster befindet sich im Kern des CUPS-Filtersystems. Er ist für die erste Stufe des Raster-Prozesses verantwortlich. Sein Input ist vom MIME-Typ application/vnd.cups-postscript; seine Ausgabe ist application/vnd.cups-raster. Dieses Ausgabeformat ist noch nicht zum Drucken gedacht, seine Aufgabe ist es, als allgemeines Input-Format für spezialisierte *Raster-Treiber* zu dienen, die imstande sind, gerätespezifische Druckerdaten zu generieren.

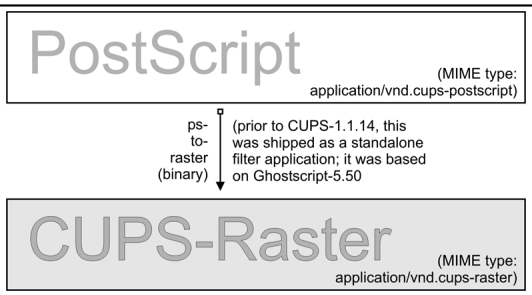


Figure 18.6. PostScript auf Übergangsraster-Format.

CUPS-Raster ist ein generisches Rasterformat mit mächtigen Eigenschaften. Es ist imstande, Informationen zu einzelnen Seiten, Farbprofile und mehr einzubeziehen, um diese Informationen nachfolgenden Raster-Treibern zu übergeben. Sein MIME-Typ ist bei der IANA registriert, und seine Spezifikation ist, natürlich, völlig offen. Es wurde entworfen, um es Herstellern zu ermöglichen, ziemlich einfach und günstig Raster-Treiber für Linux und UNIX zu entwickeln, wenn diese es möchten. CUPS übernimmt immer die erste Stufe des Rasterns, so dass Hersteller sich nicht um die Ghostscript-Komplikationen kümmern müssen (tatsächlich gibt es derzeit mehr als nur einen Hersteller, der die Entwicklung von CUPS-Raster-Treibern finanziert).

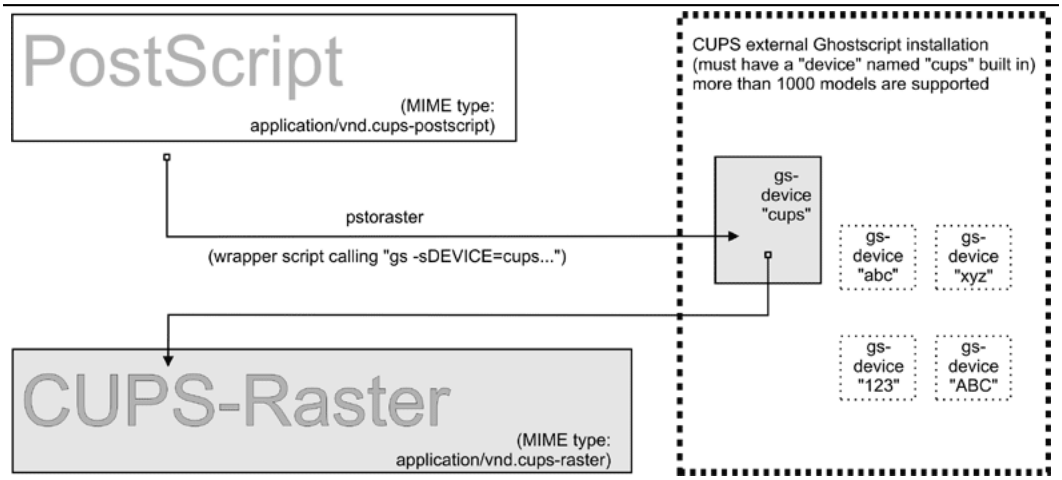


Figure 18.7. CUPS-Raster-Erzeugung mit Ghostscript

CUPS-Versionen vor Version 1.1.15 beinhalteten einen binären (oder Sourcecode-) Standalone-Filter namens *pstoraster*. *pstoraster* wurde von GNU Ghostscript 5.50 abgeleitet und konnte neben oder zusätzlich zu einem beliebigen GNU- oder AFPL-Ghostscript-Paket installiert werden, ohne Konflikte zu verursachen.

Mit Version 1.1.15 hat sich dies geändert. Die dafür benötigten Funktionen wurden zurück in Ghostscript integriert (sie basieren nun auf der GNU-Ghostscript-Version 7.05). Der *pstoraster*-Filter ist nun ein einfaches Shell-Skript, das **gs** mit dem Parameter **-sDEVICE=cups** aufruft. Wenn Ihr Ghostscript nicht erfolgreich auf **gs -h |grep cups** antwortet, könnte es sein, dass Sie nicht drucken können. Aktualisieren Sie Ihr Ghostscript.

18.4.15 imagetops und imagetoraster

Im Abschnitt über Vorfilter haben wir den Vorfilter erwähnt, der PostScript aus Bildformaten erzeugt. Der Filter *imagetoraster* wird verwendet, um Bilder direkt, ohne die Zwischenstufe PostScript, in Raster-Format zu konvertieren. Er wird öfter als die oben erwähnten Vorfilter verwendet. Wir fassen das Filtern von Bilddateien im nächsten Bild(((besser mit Abbildungsnummer))) zusammen.

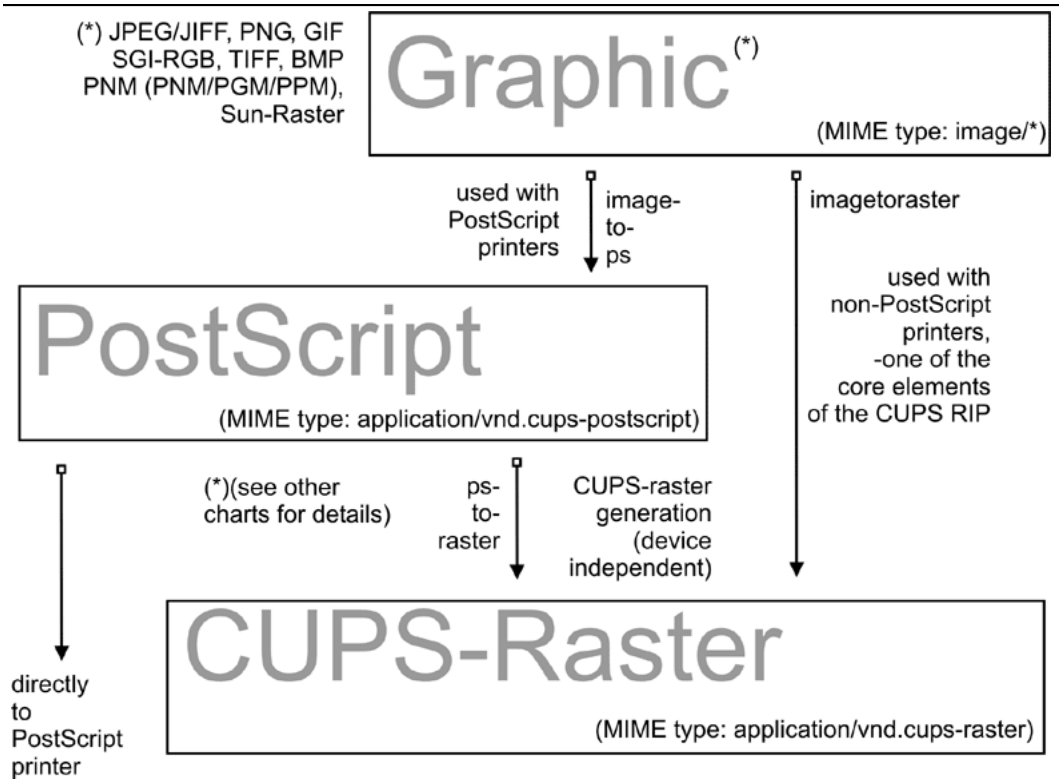


Figure 18.8. Konvertierung von Bildformaten zu CUPS-Raster-Format

18.4.16 rasterto [druckerspezifisch]

CUPS wird mit ziemlich verschiedenen Rastertreibern geliefert, die CUPS-Raster verarbeiten. Auf meinem System finde ich in /usr/lib/cups/filter/ diese: *rastertoalps*, *rastertobj*, *rastertoepson*, *rastertoescp*, *rastertopcl*, *rastertoturboprint*, *rastertoapdk*, *rastertodymo*, *rastertoescp*, *rastertohp* und *rastertoprinter*. Keine Sorge, wenn Sie weniger Filter vorfinden; manche von diesen wurden von kommerziellen CUPS-Erweiterungen installiert (wie *rastertoturboprint*), andere (wie *rastertoprinter*) von so genannten tthird-partyTreiber-Entwicklungsprojekten (wie Gimp-Print), um möglichst eng mit CUPS zusammenzuarbeiten.

18.4.17 CUPS-Backends

Der letzte Teil jeder CUPS-Filterkette ist ein Backend. Backends sind spezielle Programme, die das druckfertige Programm schlussendlich an das Gerät senden. Es gibt ein separates Backend-Programm für jedes Transfer-Protokoll, um Druckaufträge über das Netzwerk zu senden, oder für jedes lokales Interface. Jede CUPS-Druckwarteschlange braucht eine CUPS-„*device-URI*“, mit der es assoziiert wird. Die device-URI ist eine Art, das Backend codiert anzugeben, das verwendet wird, um den Auftrag an seinen Bestimmungsort zu senden.

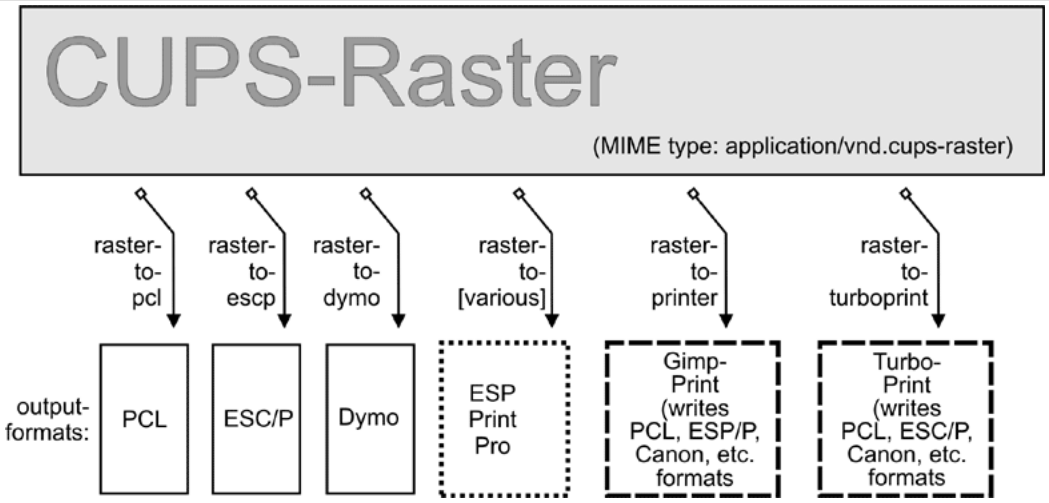


Figure 18.9. Raster auf druckerspezifische Formate

Netzwerk-device-URIs verwenden zwei Schrägstriche in ihrer Syntax, lokale device-URIs nur einen, wie Sie der folgenden Liste entnehmen können. Bitte denken Sie daran, dass die Namen der lokalen Interfaces stark von den hier angegebenen Beispielen abweichen können, wenn Ihr Betriebssystem nicht Linux ist:

usb Dieses Backend sendet Druckdateien auf Drucker, die mit USB angeschlossen sind. Ein Beispiel für die CUPS-device-URI ist: `usb:/dev/usb/lp0`.

serial Dieses Backend sendet Druckdateien auf seriell angeschlossene Drucker. Ein Beispiel für die CUPS-device-URI ist: `serial:/dev/ttyS0?baud=11500`.

parallel Dieses Backend sendet Druckdateien auf Drucker, die an Parallel-Ports angeschlossen sind. Ein Beispiel für die CUPS-device-URI ist: `parallel:/dev/lp0`.

SCSI Dieses Backend sendet Druckdateien auf Drucker, die an das SCSI-Interface angeschlossen sind. Ein Beispiel für die CUPS-device-URI ist: `scsi:/dev/sr1`.

lpd Dieses Backend sendet Druckdateien auf Netzwerk-Drücker, die über LPR/LPD angeschlossen sind. Ein Beispiel für die CUPS-device-URI ist: `lpd://remote_host_name/remote_queue_name`.

AppSocket/HP JetDirect Dieses Backend sendet Druckdateien an Netzwerk-Drucker, die mit AppSocket (alias "HP JetDirect") angeschlossen sind. Ein Beispiel für die CUPS-device-URI ist: `socket://10.11.12.13:9100`.

ipp Dieses Backend sendet Druckdateien an Netzwerk-Drucker, die mit IPP angeschlossen sind. Ein Beispiel für die CUPS-device-URI ist: `ipp://192.193.194.195/ipp` (für viele HP-Drucker) oder `ipp://remote_cups_server/printers/remote_printer_name`.

http Dieses Backend sendet Druckdateien an Drucker, die mit HTTP angeschlossen sind. (Das http://-CUPS-Backend ist nur ein symlink auf das ipp://-Backend.) Beispiele für die CUPS-device-URIs sind: `http://192.193.194.195:631/ipp` (für viele HP-Drucker) oder `http://remote_cups_server:631/printers/remote_printer_name`.

smb Dieses Backend sendet Druckdateien an Windows-Druckerfreigaben. Ein Beispiel für die CUPS-device-URI ist:

```
smb://workgroup/server/printersharename
smb://server/printersharename
smb://username:password@workgroup/server/printersharename
smb://username:password@server/printersharename
```

Das smb://-Backend ist ein Symlink auf das Samba-Werkzeug *smbspool* (nicht in CUPS enthalten). Wenn der Symlink in Ihrem CUPS-Backend-Verzeichnis nicht vorhanden ist, können Sie es als root-Benutzer anlegen (oder von root anlegen lassen): **ln -s 'which smbspool' /usr/lib/cups/backend/smb**.

Es ist einfach, Ihre eigenen Backends als Shell- oder Perl-Skripten zu schreiben, wenn Sie irgendeine Änderung oder Erweiterung zum CUPS-Druck-System brauchen. Ein Grund könnte sein, dass Sie „*spezielle*“ Drucker anlegen wollen, die Druckaufträge per E-Mail senden (durch das „*mailto:/*“-Backend), diese in PDF wandeln (durch das „*pdfgen:/*“-Backend) oder sie mittels „*/dev/null*“ entsorgen. (Tatsächlich habe ich den systemweiten Standard-Drucker so installiert, dass er mit einem devnull:/-Backend verbunden ist; es gibt einfach zu viele Leute, die Aufträge ohne Angabe eines Druckers senden oder Skripten und Programme senden, die keinen Drucker angeben. Der systemweite Standard-Drucker ?))) löscht den Auftrag und sendet eine höfliche E-Mail an den $USER, in der er gebeten wird, immer den richtigen Druckernamen anzugeben.)

Nicht alle erwähnten Backends müssen auf Ihrem System vorhanden oder verwendbar sein (abhängig von der Hardware-Konfiguration). Welche CUPS-Backends verfügbar sind, können Sie mit dem Werkzeug *lpinfo* testen. Mit der Option `-v` listet es alle verfügbaren Backends auf:

```
$ lpinfo -v
```

18.4.18 Die Rolle von cupsomatic/foomatic

cupsomatic-Filter sind wahrscheinlich die meistverwendeten Filter in CUPS-Installationen. Seien sich im Klaren darüber, dass diese Filter nicht von den CUPS-Leuten entwickelt worden sind. Es sind third partyErweiterungen für CUPS. Sie verwenden die traditionellen Ghostscript-Devices, um Aufträge für CUPS darzustellen. Bei der Fehlersuche sollten Sie

über den Unterschied Bescheid wissen. Hier findet der gesamte Darstellungsprozess in einem Schritt statt, und zwar innerhalb von Ghostscript und unter Verwendung eines passenden Gerätetreibers für den Ziel-Drucker. *cupsomatic* verwendet PPDs, die aus der Foomatic-Drucker&Treiber-Datenbank generiert werden, die Sie unter Linuxprinting.org finden.

Sie erkennen diese PPDs an der Zeile, die den *cupsomatic*-Filter aufruft:

```
*cupsFilter: "application/vnd.cups-postscript  0  cupsomatic"
```

Sie finden diese Zeile unter den ersten (ungefähr) 40 Zeilen der PPD-Datei. Wenn Sie ein solches PPD installiert haben, erscheint der Drucker im CUPS-Web-Interface mit dem Eintrag *foomatic* in der Treiberbeschreibung. *cupsomatic* ist ein Perl-Skript, das Ghostscript mit all den komplizierten Befehlszeilen-Optionen aufruft, die automatisch aus dem gewählten PPD und den Befehlszeilen-Optionen generiert wurden, die dem Druckauftrag mitgegeben wurden.

Jedoch ist *cupsomatic* mittlerweile veraltet. Seine PPDs (besonders deren erste Generation, die da draußen imer noch fleißig verwendet wird) entsprechen nicht den Adobe-Spezifikationen. Sie könnten Schwierigkeiten damit haben, wenn Sie sie mit „*Point'n'Print*“ auf Windows-Clients downloaden wollen. Ein besserer und leistungsfähigerer Nachfolger ist nun in einer stabilen Beta-Version verfügbar: Er heißt *foomatic-rip*. Um *foomatic-rip* als Filter mit CUPS zu verwenden, brauchen Sie die PPDs von neueren Typ. Diese haben eine ähnliche, jedoch andere Zeile:

```
*cupsFilter: "application/vnd.cups-postscript  0  foomatic-rip"
```

Der Mechanismus unter Linuxprinting.org, der PPDs generiert, wurde umgestaltet. Die neuen PPDs entsprechen den Adobe-Spezifikationen. Vor allem stellen sie ein neues Verfahren zur Verfügung, um mit einem einzelnen Klick verschiedene Qualitätsstufen anzugeben (hochauflösende Fotos, normale Farbe, Graustufen und Entwurf), wo Sie zuvor fünf oder mehr verschiedene Auswahlen treffen mussten (Medientyp, Auflösung, Tintenart und Dithering-Algorithmus). Es gibt Unterstützung für individuelle Mediengrößen. Es gibt Unterstützung für das Umschalten von Optionen zwischen einzelnen Seiten eines Druckauftrags. Und das Beste ist, dass der neue foomatic-rip nun nahtlos mit allen klassischen Spoolern zusammenarbeitet (wie LPRng, BSD-LPD, PDQ, PPR usw.), was diesen Spoolern die Verwendung von PPDs ermöglicht.

18.4.19 Das gesamte Bild

Wenn Sie einen Überblick über all die Filter sehen wollen und darüber, wie sie sich zueinander verhalten, finden Sie das gesamte Bild dieses Puzzles am Ende dieses Dokuments.

18.4.20 mime.convs

CUPS bildet automatisch alle möglichen Filterketten für jeden beliebigen MIME-Typ und jeden installierten Drucker. Aber wie entscheidet es sich für oder gegen eine bestimmte

Alternative? (Es kann oft Fälle geben, in denen es zwei oder mehr Filterketten für denselben Ziel-Drucker gibt.) Das ist einfach. Sie haben vielleicht die Zahlen in der dritten Spalte der Datei mime.convs bemerkt. Diese repräsentieren virtuelle Kosten, die dem jeweiligen Filter zugeordnet sind. Jede mögliche Filterkette ergibt eine Summe von „*Filter-Kosten.*“ CUPS entscheidet zugunsten der „*günstigsten*“ Route.

TIPP

Die Einstellung von *FilterLimit 1000* in cupsd.conf bewirkt, dass nur so viele Filter gleichzeitig ausgeführt werden, dass sie insgesamt 1000 virtuelle Filter-Kosten verursachen. Dies ist eine effiziente Art, die Last eines CUPS-Servers zu begrenzen, indem man einen passenden Wert für „*FilterLimit*“ setzt. Ein FilterLimit von 200 erlaubt nur ungefähr einen Auftrag zur gleichen Zeit, während ein FilterLimit von 1000 ungefähr fünf Aufträge gleichzeitig erlaubt.

18.4.21 „*Raw*“-Druck

Sie können CUPS (so ziemlich) jede Datei „*raw*“ drucken lassen. „*Raw*“ bedeutet, dass sie nicht gefiltert wird. CUPS sendet die Datei so an den Drucker, „*wie sie ist*“, ohne sich darum zu kümmern, ob der Drucker imstande ist, diese Datei zu „*verdauen*“. Die Benutzer müssen sich selbst darum kümmern, dass sie nur sinnvolle Datenformate senden. Raw-Druck kann in jeder Warteschlange stattfinden, wenn die Option „*-o raw*“ auf der Befehlszeile angegeben wird. Sie können auch Nur-raw-Queues anlegen, indem Sie einfach keinerlei PPD mit einer Queue assoziieren. Der Befehl

```
$ lpadmin -P rawprinter -v socket://11.12.13.14:9100 -E
```

installiert eine Queue namens „*rawprinter*“, die über das Protokoll „*socket*“ (alias „*HP JetDirect*“) mit dem Gerät mit der IP-Adresse 11.12.1.3.14 verbunden ist, das an Port 9100 arbeitet. (Wenn Sie ein PPD mit **-P /path/to/PPD** zur Befehlszeile hinzugefügt hätten, hätten Sie eine „*normale*“ Druck-Queue installiert.)

CUPS behandelt automatisch jeden Auftrag, der an eine Queue gesendet wird, als „*raw*“, wenn es keine mit der Queue assoziierte PPD vorfindet. Jedoch wird CUPS nur bekannte MIME-Typen senden (wie in seiner eigenen Datei mime.types definiert) und andere ablehnen.

18.4.22 application/octet-stream-Druck

Jeder MIME-Typ ohne Regel in der Datei /etc/cups/mime.types wird als unbekannt oder als *application/octet-stream* betrachtet und nicht gesendet. Weil CUPS es standardmäßig ablehnt, unbekannte MIME-Typen zu drucken, haben Sie vielleicht schon einmal

erlebt, dass Druckaufträge von Windows-Clients nicht gedruckt wurden. Sie haben vielleicht eine Fehlermeldung in Ihren CUPS-Logdateien gefunden, die wie folgt lautete:

```
Unable to convert file 0 to printable format for job
```

Um das Drucken von Dateien des Typs *application/octet-stream* zu ermöglichen, müssen Sie zwei Dateien editieren:

- `/etc/cups/mime.convs`
- `/etc/cups/mime.types`

Beide enthalten Einträge (am Ende der jeweiligen Datei), die auskommentiert werden müssen, um RAW-Verarbeitung des MIME-Typs *application/octet-stream* zu erlauben. In `/etc/cups/mime.types` muss diese Zeile vorhanden sein:

```
application/octet-stream
```

Diese Zeile (ohne spezifisches (((auto-typing rule set)))? ordnet alle Dateien, die nicht anderswo automatisch typisiert wurden, dem Typ *application/octet-stream* zu. Stellen Sie sicher, daß Sie in `/etc/cups/mime.convs` folgende Zeile haben:

```
application/octet-stream   application/vnd.cups-raw   0   -
```

Diese Zeile weist CUPS an, für den MIME-Typ *application/octet-stream* den *Null-Filter* zu verwenden (markiert mit „-“, tut gar nichts) und das Resultat als *application/vnd.cups-raw* zu kennzeichnen. Dies ist immer ein grünes Licht für den CUPS-Scheduler, um die Datei an das Backend zu übergeben, das sich dann mit dem Drucker verbindet und die Datei sendet.

ANMERKUNG

Das Editieren von `mime.convs` und `mime.types` *erzwingt* den „*raw*“-Druck nicht, es *erlaubt* ihn nur.

Hintergrund. Da CUPS ein sicherheitsbewussteres Drucksystem ist als die traditionellen Systeme, erlaubt es per Voreinstellung nicht, dass ein Benutzer beliebige (möglicherweise binäre) Daten an Druckgeräte sendet. (Dies könnte leicht dazu benutzt werden, einen „*Denial of Service*“-Angriff auf Ihre(n) Drucker zu starten, was zumindest den Verlust von einer Menge Papier und Tinte nach sich ziehen würde.) „*Unbekannte*“ Daten werden von CUPS als *MIME-Typ application/octet-stream* behandelt. Sie *können* zwar Daten „*raw*“ senden, aber der MIME-Typ für diese Daten muss einer sein, der CUPS bekannt und erlaubt ist. Die Datei `/etc/cups/mime.types` legt die Regeln fest, wie CUPS MIME-Typen erkennt. Die Datei `/etc/cups/mime.convs` entscheidet, welche Umwandlungsfilter auf welche MIME-Typen angewandt werden können.

18.4.23 PostScript Printer Descriptions (PPDs) für Nicht-PS-Drucker

Ursprünglich waren PPDs nur zur Verwendung mit PostScript-Druckern gedacht. Hier helfen sie dabei, gerätespezifische Befehle und Einstellungen an den RIP zu senden, der die Auftragsdatei verarbeitet. CUPS hat die Reichweite von PPDs erweitert, um auch Nicht-PS-Drucker abzudecken. Dies war nicht schwierig, da es ein standardisiertes Dateiformat ist. Auf eine gewisse Art war es auch logisch: CUPS verarbeitet PostScript und verwendet einen PostScript-RIP (Ghostscript), um die Auftragsdateien zu verarbeiten. Der einzige Unterschied ist: Ein PostScript-Drucker hat den RIP eingebaut, für die anderen Arten von Drucker läuft der Ghostscript-RIP auf dem Druck-Server.

PPDs für einen Nicht-PS-Drucker beinhalten ein paar Zeilen, die einzigartig für CUPS sind. Die wichtigste sieht ungefähr so aus:

```
*cupsFilter: application/vnd.cups-raster  66   rastertoprinter
```

Dies ist das letzte Stück im CUPS-Filter-Puzzle. Diese Zeile weist den CUPS-Daemon an, als letzten Filter *rastertoprinter* zu verwenden. Dieser Filter sollte als Input eine Datei vom MIME-Typ *application/vnd.cups-raster* serviert bekommen. Daher sollte CUPS automatisch eine Filterkette konstruieren, die als letzte Ausgabe den angegebenen MIME-Typ liefert. Diese wird dann als Input für den erwähnten Filter *rastertoprinter* verwendet. Nachdem der letzte Filter seine Arbeit getan hat (*rastertoprinter* ist ein Gimp-Print-Filter), sollte die Datei an das Backend gesendet werden, das sie anschließend an das Ausgabe-Gerät sendet.

CUPS liefert standardmäßig nur ein paar generische PPDs, aber diese können für ein paar hundert Drucker-Modelle verwendet werden. Es kann sein, dass Sie damit nicht verschiedene Papierschächte verwalten können oder dass Sie breitere Druckränder erhalten, als Ihr spezielles Modell unterstützt. Die Tabelle Mit CUPS gelieferte PPDs(((Nummerierung?))) zeigt eine Zusammenfassung.

Tabelle 18.1. Mit CUPS gelieferte PPDs

PPD-Datei	Drucker-Typ
deskjet.ppd	ältere HP-Inkjet-Drucker und Kompatible
deskjet2.ppd	neuere HP-Inkjet-Drucker und Kompatible
dymo.ppd	Label-Drucker
epson9.ppd	Epson-9pin-Nadeldrucker und Kompatible
epson24.ppd	Epson-24pin-Nadeldrucker und Kompatible
okidata9.ppd	Okidata-9pin-Nadeldrucker und Kompatible
okidat24.ppd	Okidata-24pin-Nadeldrucker und Kompatible
stcolor.ppd	ältere Epson Stylus Color-Drucker
stcolor2.ppd	neuere Epson Stylus Color-Drucker
stphoto.ppd	ältere Epson Stylus Photo-Drucker
stphoto2.ppd	neuere Epson Stylus Photo-Drucker
laserjet.ppd	alle PCL-Drucker. Weiter unten finden Sie mehr über einige andere Treiber/PPD-Pakete, die für die Verwendung mit CUPS geeignet sind.

18.4.24 *cupsomatic/foomatic-rip* versus *nativer CUPS*-Druck

Natives CUPS-Rastern arbeitet in zwei Schritten:

- Zuerst kommt der Schritt ***pstoraster***. Dieser verwendet das spezielle CUPS-device aus ESP Ghostscript 7.05.x als Werkzeug.
- Als zweites kommt der Schritt ***rasterdriver***. Er verwendet gerätespezifische Filter; es gibt einige Hersteller, die Filter guter Qualität für diesen Schritt zur Verfügung stellen. Manche sind freie Software, andere Shareware bzw. nicht-frei, manche proprietär.

Oft erzeugt dies bessere Qualität (und hat einige Vorteile mehr) als andere Methoden.

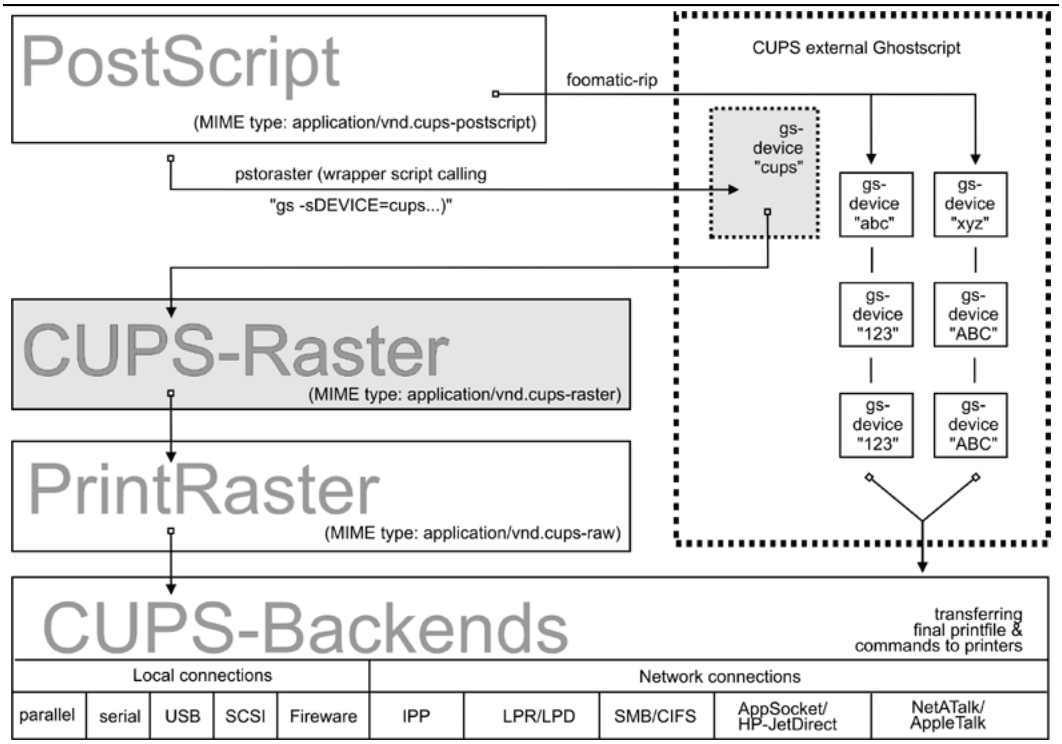


Figure 18.10. cupsomatic/foomatic Verarbeitung versus nativem CUPS.

Eine andere Methode ist der Weg über ***cupsomatic/foomatic-rip***. Beachten Sie, dass ***cupsomatic*** *nicht* von den CUPS-Leuten geschrieben wird. cupsomatic ist ein unabhängiger Beitrag zur Entwicklung des Druckens von den Leuten von Linuxprinting.org [1]. ***cupsomatic*** wird nicht mehr entwickelt, gewartet oder unterstützt. Es wurde durch ***foomatic-rip*** ersetzt. ***foomatic-rip*** ist eine komplette Neufassung der alten Idee von ***cupsomatic***, aber sehr stark verbessert und generalisiert, um andere (Nicht-CUPS-) Spooler zu unterstützen. Ein Upgrade auf foomatic-rip wird wärmstens empfohlen, besonders wenn Sie auf eine aktuelle Version von CUPS aktualisieren.

[1] sehen Sie auch <`http://www.cups.org/cups-help.html`>

Sowohl die Methode *cupsomatic* (alt) als auch die Methode *foomatic-rip* (neu) von Linuxprinting.org verwenden die traditionelle Ghostscript-Verarbeitung von Druckdateien, die alles in einem Schritt erledigt. Sie hängt davon ab, dass all die anderen Geräte bereits in Ghostscript eingebaut sind. Die Qualität ist so gut (oder schlecht), wie die Ghostscript-Darstellung in den anderen Spoolern ist. Der Vorteil ist, dass diese Methode viele Drucker-Modelle unterstützt, die (noch) nicht von der moderneren CUPS-Methode unterstützt werden.

Natürlich können Sie beide Methoden nebeneinander auf einem System einsetzen (und sogar auf einem Drucker, wenn Sie verschiedene Queues installieren) und herausfinden, welche am besten für Sie funktioniert.

cupsomatic "kidnappt" die Druckdatei nach der Stufe *application/vnd.cups-postscript* und lenkt sie durch die CUPS-externe, systemweite Ghostscript-Installation um. Daher umgeht die Druckdatei den Filter *pstoraster* (und umgeht auch die CUPS-Raster-Treiber *rastertosomething*). Nachdem Ghostscript sein Rastern beendet hat, übergibt *cupsomatic* die dargestellte Datei direkt an das CUPS-Backend. Das Flussdiagramm in cupsomatic/foomatic-Verarbeitung versus natives CUPS(((Nummerierung?))) illustriert den Unterschied zwischen der nativen CUPS-Darstellung und der *Foomatic/cupsomatic*-Methode.

18.4.25 Beispiele für Filterketten

Es folgen ein paar Beispiele für gängige Filterketten, um die Funktion von CUPS zu illustrieren.

Nehmen wir an, Sie wollen eine PDF-Datei auf einem per HP JetDirect angeschlossenen PostScript-Drucker drucken, aber Sie wollen nur die Seiten 3-5, 7, 11-13 drucken, und das mit „*two-up*“ und „*Duplex*“:

- Ihre Druck-Optionen (Seitenauswahl, two-up, Duplex) werden über die Befehlszeile an CUPS weitergegeben.
- Die (komplette) PDF-Datei wird an CUPS gesendet und automatisch als *application/pdf* typisiert.
- Die Datei muss daher zuerst den Vorfilter *pdftops* passieren, der den PostScript MIME-Typ *application/postscript* erzeugt (eine Vorschau an dieser Stelle würde immer noch alle Seiten des originalen PDFs zeigen).
- Die Datei passiert sodann den Filter *pstops*, der die Befehlszeilen-Optionen anwendet: Er wählt die Seiten 3-5, 7 und 11-13, legt ein Layout mit „*zwei Seiten pro Blatt*“ an und fügt den korrekten Befehl für „*Duplex*“ (wie im PPD des Druckers definiert) in die PostScript-Datei ein; die Datei ist jetzt vom PostScript-MIME-Typ *application/vnd.cups-postscript*.
- Die Datei geht jetzt an das *socket*-Backend, das den Auftrag an die Drucker weiterleitet.

Die daraus resultierende Filterkette ist in Filterkette PDF auf socket(((Abbildungsnummer?))) dargestellt.

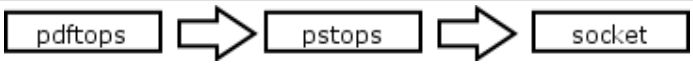


Figure 18.11. Filterkette PDF auf socket

Nehmen wir an, Sie wollen aus demselben Filter auf einen an USB angeschlossenen Epson Stylus Photo-Drucker drucken, der mit dem CUPS-PPD `stphoto2.ppd` installiert wurde. Die ersten paar Filter-Stufen sind fast dieselben:

- Ihre Druck-Optionen (Seitenauswahl, two-up, Duplex) werden per Befehlszeile an CUPS weitergegeben.
- Die (komplette) PDF-Datei wird an CUPS gesendet und automatisch als *application/pdf* typisiert.
- Die Datei muss daher zuerst den Vorfilter *pdftops* passieren, der den PostScript MIME-Typ *application/postscript* erzeugt (eine Vorschau an dieser Stelle würde immer noch alle Seiten des originalen PDFs zeigen).
- Die Datei passiert sodann den Filter *pstops*, der die Befehlszeilen-Optionen anwendet: Er wählt die Seiten 3-5, 7 und 11-13, legt ein Layout mit „*2 Seiten pro Blatt*“ an und fügt den korrekten Befehl für „*Duplex*“ ... (hoppla — dieser Drucker und diese PPD unterstützen gar keinen Duplex-Druck — also wird diese Option ignoriert) in die PostScript-Datei ein; die Datei ist jetzt vom PostScript-MIME-Typ *application/vnd.cups-postscript*.
- Die Datei passiert jetzt die Filter-Stufe *pstoraster* und wird zum MIME-Typ *application/cups-raster*.
- Zuletzt tut der Filter *rastertoepson* seine Arbeit (wie in der PPD des Druckers angezeigt), legt die drucker-spezifischen Rasterdaten an und bettet alle vom Benutzer gewählten Druck-Optionen in die Druckdaten ein.
- Die Datei geht an das Backend *usb*, das es an die Drucker weiterleitet.

Die daraus resultierende Filterkette ist in diesem Bild(((Abbildungsnummer))) dargestellt.

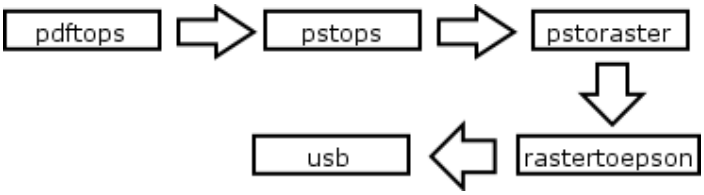


Figure 18.12. Filterkette PDF auf USB

18.4.26 Quellen für CUPS-Treiber/PPDs

Im Internet finden Sie viele tausend CUPS-PPD-Dateien (mit ihren begleitenden Filtern) in vielen Landessprachen und mit Unterstützung für über tausend Nicht-PostScript-Modelle.

- ESP PrintPro <http://wwwl.easysw.com/printpro/> (kommerziell, nicht frei) wird mit mehr als 3000 PPDs gebündelt. Sie können es „*out of the box*“ auf Linux, Mac OS X, IBM-AIX, HP-UX, Sun-Solaris, SGI-IRIX, Compaq Tru64, Digital UNIX und noch einigen kommerziellen UNIX-Versionen verwenden. (Es wurde von den CUPS-Entwicklern selbst geschrieben und sein Verkauf hilft niht nur dabei, die weitere Entwicklung von CUPS zu finanzieren, sondern ernährt auch dessen Schöpfer.)
- Das Gimp-Print-Project <http://gimp-print.sourceforge.net/> (GPL, freie Software) bietet ungefähr 140 PPDs (mit Unterstützung von fast 400 Druckern, viele davon bis zu Foto-Qualität), die neben den Gimp-Print-CUPS-Filtern genutzt werden können.
- TurboPrint <http://www.turboprint.com/> (Shareware, nicht frei) unterstützt ungefähr dieselbe Anzahl von Druckern in exzellenter Qualität.
- OMNI <http://www-124.ibm.com/developerworks/oss/linux/projects/omni/> (LPGL, frei) ist ein Package von IBM, das mittlerweile Unterstützung für mehr als 400 Drucker enthält. Es stammt aus dem Erbe des IBM OS/2-Know-how, das auf Linux portiert wurde (die CUPS-Unterstützung ist derzeit im Beta-Stadium).
- HPIJS <http://hpinkjet.sourceforge.net/> (BSD-artige Lizenz, frei) unterstützt ungefähr 150 Drucker von HP und bietet nun auch exzellente Druckqualität (derzeit nur über den Foomatic-Pfad verfügbar).
- Foomatic/cupsomatic <http://www.linuxprinting.org/> (LPGL, frei) von Linuxprinting.org bietet PPDs für praktisch jeden auf der Welt bekannten Ghostscript-Filter (einschließlich Omni, Gimp-Print und HPIJS).

18.4.27 Das Drucken mit Interface Scripts

CUPS unterstützt auch die Verwendung von „*interface scripts*“, wie man sie von System V-AT&T-Drucksystemen kennt. Diese werden oft für PCL-Drucker verwendet, und zwar von Anwendungen, die PCL-Druckaufträge erzeugen. Interface scripts sind für einzelne Drucker-Modelle spezifisch. Sie haben eine ähnliche Rolle wie PPDs für PostScript-Drucker. Interface scripts können die benötigten Escape-Sequenzen in den Druck-Datenstrom einfügen, wenn der Benutzer einen bestimmten Papierschacht gewählt hat, oder Landscape-Druck oder A3-Papier etc. Interface scripts sind in der Linux-Welt praktisch unbekannt. Auf HP-UX-Plattformen werden sie öfter verwendet. Sie können jedes funktionierende interface script auch mit CUPS verwenden. Installieren Sie einfach den Drucker mit der Option **-i**:

```
root# lpadmin -p pclprinter -v socket://11.12.13.14:9100 \
  -i /path/to/interface-script
```

Interface scripts sind vielleicht eine „*unbekannte Größe*“ für viele. Nichtsdestotrotz bieten sie mit CUPS den einfachsten Weg, Ihr eigenes selbst geschriebenes Filter-Skript oder -Programm in eine bestimmte Drucker-Queue einzufügen (einige Informationen über die herkömmliche Verwendung von interface scripts können Sie unter <http://playground.sun.com/printing/documentation/interface.html> finden.

18.5 Netzwerk-Druck (ausschließlich Windows)

Netzwerk-Druck umfasst ein weites Feld. Um zu verstehen, was genau mit Samba passiert, wenn es im Auftrag seiner Windows-Clients druckt, lassen Sie uns zuerst einen Blick auf ein „*reines Windows*“-Setup werfen: Windows-Clients mit einem Windows NT Druck-Server.

18.5.1 Von Windows-Clients auf einen NT-Druck-Server drucken

Windows-Clients, die auf einen NT-basierenden Druck-Server drucken, haben zwei Möglichkeiten. Sie können:

- den Treiber lokal ausführen und die GDI-Ausgabe (EMF) selbst im druckerspezifischen Format darstellen.
- die GDI-Ausgabe (EMF) an den Server senden, wo der Treiber ausgeführt wird, um die druckerspezifische Ausgabe darzustellen.

Die beiden Druck-Möglichkeiten werden in den Flussdiagrammen Treiberausführung auf dem Client und Treiberausführung auf dem Server gezeigt.

18.5.2 Treiberausführung auf dem Client

Im ersten Fall muss der Druck-Server die Datei als raw behandeln. Das bedeutet, er sollte die Auftragsdatei nicht anrühren oder in irgendeiner Art zu konvertieren versuchen. Dies ist, was ein herkömmlicher UNIX-basierender Druck-Server auch tun kann, und das bei besserer Performance und stabiler als ein NT-Druck-Server. Damit sind wohl die meisten Samba-Administratoren vertraut. Ein Vorteil dieses Setups ist, dass dieser „*spooling-only*“-Druck-Server sogar verwendet werden kann, wenn kein(e) Treiber für UNIX verfügbar sind. Es genügt, die Windows-Treiber zur Verfügung und auf den Clients installiert zu haben.

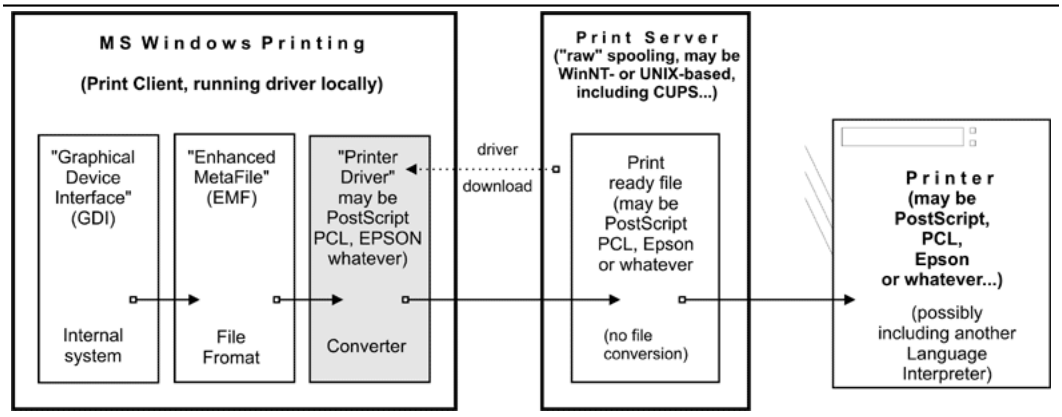


Figure 18.13. Treiberausführung auf dem Client

18.5.3 Treiberausführung auf dem Server

Der andere Pfad führt den Druckertreiber auf dem Server aus. Der Client übermittelt Druckdateien im EMF-Format an den Server. Der Server verwendet den PostScript-, PCL-, ESC/P- oder einen anderen Treiber, um die EMF-Datei in die druckerspezifische Sprache zu konvertieren. Es ist UNIX nicht möglich, dasselbe zu tun. Derzeit gibt es kein Programm und keine Methode, um die GDI-Ausgabe eines Windows-Clients auf einem UNIX-Server auf etwas umzuwandeln, das ein Drucker verstehen könnte.

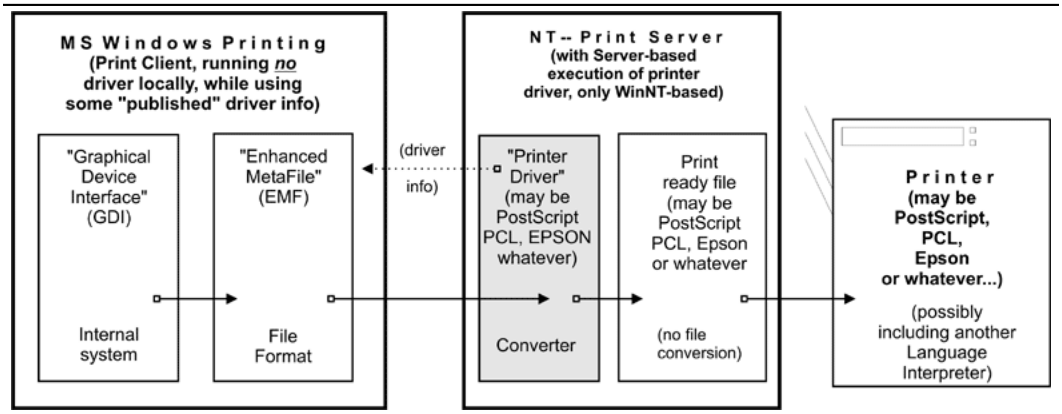

MS Windows Printing
(Print Client, running no driver locally, while using some "published" driver info)
"Graphical Device Interface" (GDI)
"Enhanced MetaFile" (EMF)
Internal system
File Format
(driver info)
NT-- Print Server
(with Server-based execution of printer driver, only WinNT-based)
"Printer Driver" (may be PostScript PCL, EPSON whatever)
Converter
Print ready file (may be PostScript PCL, Epson or whatever
(no file conversion)
Printer
(may be PostScript, PCL, Epson or whatever...)
(possibly including another Language Interpreter)

Figure 18.14. Treiberausführung auf dem Server

Jedoch ist etwas Ähnliches mit CUPS möglich. Lesen Sie weiter.

18.6 Netzwerk-Druck (Windows-Clients — UNIX/Samba-Druck-Server)

Da UNIX-Server den Win32-Programmcode *NICHT* auf ihrer Plattform ausführen können, ist die Sache etwas anders. Dies schränkt jedoch Ihre Möglichkeiten nicht allzu sehr ein. Im Gegenteil, Sie haben hier die Möglichkeit, Druckoptionen zu implementieren, die anderswo nicht möglich sind.

18.6.1 Von Windows-Clients auf einen CUPS/Samba-Druck-Server drucken

Hier ist ein einfaches Rezept, das zeigt, wie Sie zum Nutzen Ihrer druckenden Windows-Clients Vorteile aus den mächtigen Eigenschaften von CUPS ziehen:

- Lassen Sie die Windows-Clients PostScript an den CUPS-Server senden.
- Lassen Sie den CUPS-Server das PostScript in ein gerätespezifisches Format wandeln.

Dies erfordert, dass die Clients einen PostScript-Treiber verwenden (sogar, wenn der Drucker kein PostScript-Modell ist). Es erfordert auch, dass Sie einen Treiber auf dem CUPS-Server haben.

Um CUPS-basierendes Drucken per Samba zu aktivieren, sollten zunächst folgende Optionen im Abschitt [global] Ihrer Datei `smb.conf` gesetzt werden:

```
printing = cups
printcap = cups
```

Wenn diese Parameter angegeben werden, werden alle manuell gesetzten Druck-Anweisungen (wie print command oder lppause command) in `smb.conf` (genauso wie in Samba selbst) ignoriert. Stattdessen arbeitet Samba direkt mit CUPS zusammen. Dazu verwendet es dessen äpplication program interface"(API), sofern Samba mit Unterstützung der CUPS-Bibliothek (libcups) kompiliert wurde. Wenn Samba nicht mit CUPS-Unterstützung kompiliert wurde und wenn keine anderen Druckbefehle gesetzt sind, wird der Druck den *System V*-AT&T-Befehlssatz mit der automatisch gesetzten Option „*-oraw*“ verwenden, womit Druckaufträge einfach weitergegeben werden. (Wenn Sie Ihre selbst definierten Druckbefehle mit einem Samba-Server verwenden wollen, der CUPS-Unterstützung einkompiliert hat, verwenden Sie einfach printing = sysv.)

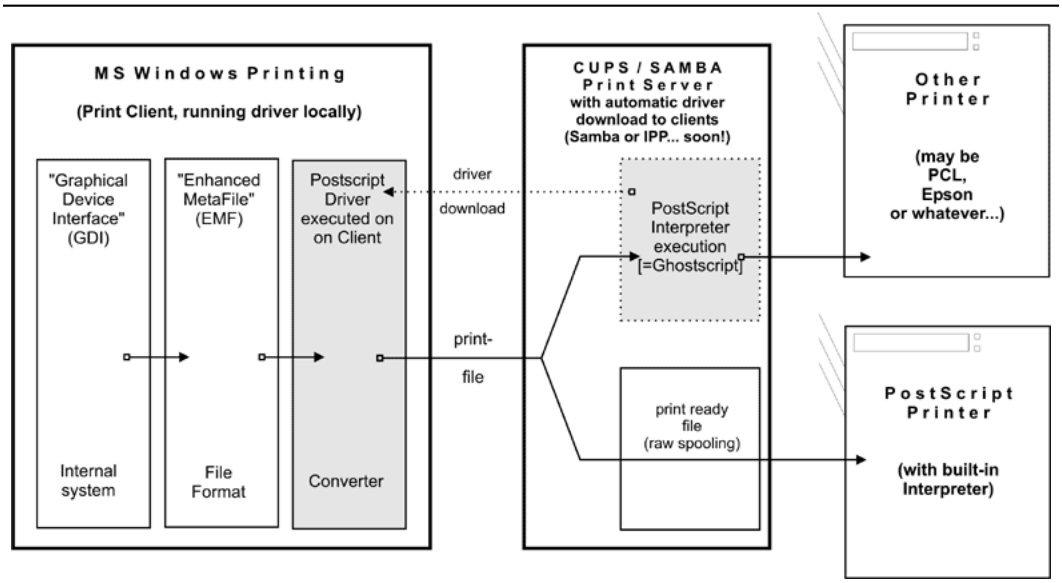


Figure 18.15. Drucken über einen CUPS/Samba-Server

18.6.2 Samba empfängt Aufträge und gibt sie an CUPS weiter

Samba *muss* sein eigenes Spooling-Verzeichnis verwenden. (Es wird mit einer Zeile wie path = /var/spool/samba im Abschnitt *[printers]* oder *[printername]* von `smb.conf` gesetzt.) Samba empfängt den Auftrag in seinem eigenen Spooling-Verzeichnis und leitet ihn in das Spooling-Verzeichnis von CUPS weiter. (Das CUPS-Spooling-Verzeichnis wird mit der Anweisung *RequestRoot* in einer Zeile gesetzt, die per Voreinstellung *RequestRoot /var/spool/cups* lautet). CUPS prüft die Zugriffsrechte und setzt diese bei jdem Neustart auf vernünftige Werte. Wir haben schon ziemlich viele Leute gesehen, die ein gemeinsames

Spooling-Verzeichnis verwendet haben und wochenlang mit diesem „*Problem*“ zu kämpfen hatten.

Ein Windows-Benutzer authentifiziert sich nur gegenüber Samba (mittels dessen, was konfiguriert wurde). Wenn Samba auf demselben Host wie CUPS läuft, brauchen Sie nur dem Rechner „*localhost*“ das Drucken zu erlauben. Wenn Samba und CUPS auf verschiedenen Maschinen laufen, müssen Sie sicherstellen, dass der Samba-Host Zugriff auf das Drucken auf CUPS hat.

18.7 Netzwerk-PostScript-RIP

Dieser Abschnitt behandelt die Verwendung von CUPS-Filtern auf der Server-Konfiguration, in der Clients einen PostScript-Treiber mit CUPS-PPDs verwenden.

PPDs können alle Optionen des Drucker-Geräts kontrollieren. Sie werden üblicherweise vom Hersteller bereitgestellt, wenn Sie einen PostScript-Drucker besitzen. PPD-Dateien (PostScript Printer Descriptions) sind immer Bestandteil der Druckertreiber auf MS Windows- oder Apple Mac OS-Systemen. Es sind ASCII-Dateien, die vom Benutzer wählbare Druckoptionen sowie deren Zuweisung auf die enstprechenden PostScript-, PCL- oder PJL-Befehle für das Ziel-Gerät enthalten. Die GUI-Dialoge der Druckertreiber übersetzen diese Optionen „*on-the-fly*“ in Schaltflächen und Auswahllisten, um dem Benutzer eine Auswahl anzubieten.

CUPS kann ohne jede Umwandlung PPD-Dateien von jedem Windows-PS-Treiber (NT wird empfohlen) und dessen Optionen verarbeiten. Es gibt ein Web-Interface zu den Druck-Optionen (gehen Sie auf <`http://localhost:631/printers/`>, und klicken Sie auf eine **Configure Printer**-Schaltfläche) oder ein Befehlszeilen-Interface (sehen Sie dazu **man lpoptions**, oder prüfen Sie, ob Sie **lphelp** auf Ihrem System haben). Es gibt auch ein paar verschiedene GUI-Frontends für Linux/UNIX, die PPD-Optionen darstellen können. PPD-Optionen sind normalerweise zur Interpretation durch den PostScript-RIP auf dem PostScript-Drucker gedacht.

18.7.1 PPDs für Nicht-PS-Drucker auf UNIX

CUPS beschränkt sich in seiner Verwendung von PPDs nicht auf „*wirkliche*“ PostScript-Drucker. Die CUPS-Entwickler haben die Reichweite des PPD-Konzepts erweitert, um auch verfügbare Geräte- und Treiber-Optionen von Nicht-PS-Druckern durch CUPS-PPDs zu beschreiben.

Dies ist nur logisch, da CUPS einen voll ausgestatteten PostScript Interpreter (RIP) umfasst. Dieser RIP basiert auf Ghostscript. Er kann alles empfangene PostScript (und zusätzlich viele weitere Dateiformate) verarbeiten. Alle CUPS-PPDs für Nicht-PS-Drucker enthalten eine zusätzliche Zeile, die mit dem Schlüsselwort `*cupsFilter` beginnt. Diese Zeile teilt dem CUPS-Druck-System mit, welcher druckerspezifische Filter zur Interpretation der PostScript-Daten verwendet werden soll. Daher lässt CUPS alle seine Drucker für die Clients als PostScript-Drucker erscheinen, weil es als PostScript-RIP für diese Drucker arbeiten kann.

18.7.2 PPDs für Nicht-PS-Drucker auf Windows

CUPS-PPDs können auch auf Windows-Clients verwendet werden, auf dem „*Rücken*“ eines „*core*“-PostScript-Treibers (derzeit wird der CUPS PostScript Driver for Windows NT/200x/XPëmpfohlen; Sie können auch den von Adobe verwenden, allerdings mit Einschränkungen). Dieses Feature ermöglicht es CUPS, einige Tricks zu beherrschen, die kein anderer Spooler kann:

- Das Arbeiten als ein vernetzter PostScript RIP-(Raster Image Processor), der Druckdateien von allen Client-Plattformen in einer einheitlichen Weise handhabt.
- Das Arbeiten als zentraler Ab- und Verrechnungsserver, da alle Dateien durch den pstops-Filter laufen und daher in der CUPS-Datei `page_log` protokolliert werden. *Anmerkung:* Dies kann nicht für „*raw*“-Druckaufträge erfolgen, da diese ja per definitionem ungefiltert bleiben.
- Das Ermöglichen einer Einigung und Festlegung eines einzelnen PostScript-Treibers für die Clients, sogar für viele verschiedene Ziel-Drucker.

Die Verwendung von CUPS-PPDs auf Windows-Clients ermöglicht es diesen, alle Druckauftragseinstellungen so zu kontrollieren, wie es ein UNIX-Client kann.

18.8 Windows Terminal Server (WTS) als CUPS-Clients

Dieses Setup wird für diejenigen interessant sein, die große Probleme in WTS-Umgebungen haben. In WTS muss oft eine Vielzahl von Nicht-PS-Treibern installiert sein, um die Vielfalt der verschiedenen Druckermodelle der Clients zu unterstützen. Dies bringt oft eine stark erhöhte Instabilität mit sich.

18.8.1 Drucker-Treiber, die im „*Kernel-Modus*“ laufen, verursachen viele Probleme

In Windows NT bringen Drucker-Treiber, die im „*Kernel-Modus*“ laufen, ein hohes Risiko für die Stabilität des Systems mit sich, wenn der Treiber nicht wirklich stabil und gut getestet ist. Und es gibt eine Menge schlechte Treiber! Speziell berüchtigt ist das Beispiel des PCL-Drucker-Treibers, der ein zusätzliches Sound-Modul ausführte, das die Benutzer via Soundkarte über ihre abgeschlossenen Druckaufträge informierte. Muss ich wirklich erwähnen, dass dies genauso verlässlich „*blue screens of death*“ verursachte?

PostScript-Treiber sind im Allgemeinen gut getestet. Sie sind nicht dafür bekannt, irgendwelche Probleme zu verursachen, sogar obwohl sie auch im Kernel-Modus ausgeführt werden. Das kann daher kommen, dass es bislang nur zwei verschiedene PostScript-Treiber gab: die von Adobe und den von Microsoft. Beide sind gut getestet und so stabil, wie es unter Windows eben geht. Der CUPS-Treiber ist von dem MS-Treiber abgeleitet.

18.8.2 Workarounds bringen massive Einschränkungen

In vielen Fällen haben Administratoren in dem Bestreben, dieses Problem zu umgehen, die erlaubten Druckertreiber auf ihrem WTS auf einen generischen PCL- und einen PostScript-

Treiber beschränkt. Dies schränkt jedoch die Clients im Umfang der ihnen zur Verfügung stehenden Druckoptionen ein. Oft bekommen Sie nicht mehr als Simplex-Druck aus einem Standard-Papierschacht, während Ihre Geräte bei weitem mehr könnten, wenn sie von einem besseren Treiber angesteuert würden!

18.8.3 CUPS: Ein „*Stein der Weisen*“?

Das Verwenden eines Postscript-Treibers, der mit einem CUPS-PPD aktiviert wurde, scheint eine sehr elegante Art zu sein, all diese Mängel zu überbrücken. Es gibt, je nach der von Ihnen verwendeten Windows-Version, bis zu drei verschiedene verfügbare Postscript-Treiber: Adobe, Microsoft und CUPS-Postscript-Treiber. Keiner der drei ist bekannt dafür, größere Instabilitäten auf WTS zu verursachen (auch nicht, wenn viele verschiedene PPDs verwendet werden). Die Clients werden (wieder) imstande dazu sein, Papierschächte auszuwählen, Duplexdruck und andere Einstellungen auszuführen. Dies hat jedoch auch seinen Preis: Ein CUPS-Server, der als PostScript-RIP für seine Clients arbeitet, erfordert mehr CPU und RAM, als wenn er nur als „*raw spooling*“-Server arbeitet. Außerdem ist dieses Setup noch nicht ausführlich getestet, wobei die ersten Rückmeldungen sehr vielversprechend aussehen.

18.8.4 PostScript-Treiber ohne größere Probleme — sogar im Kernel-Modus

Aktuellere Drucker-Treiber unter W200x und XP laufen nicht mehr im Kernel-Modus (anders als unter Windows NT). Beide Betriebssysteme können jedoch die NT-Treiber verwenden, die im Kernel-Modus laufen. (Sie können grob bestimmen, welcher Treiber zu welchem System gehört, da die Treiber im Unterverzeichnis „*2*“ des Verzeichnisses „*W32X86*“ die „*alten*“ sind.) Wie zuvor gesagt wurde, sind weder die Adobe-Treiber noch die von MS dafür bekannt, irgendwelche Stabilitätsprobleme zu verursachen. Der CUPS-Treiber wurde vom MS-Treiber abgeleitet. Es gibt einen einfachen Grund dafür: Das MS DDK (Device Development Kit) für Windows NT (das für Lizenznehmer von Visual Studio ohne Kosten verfügbar war) beinhaltet den Quelltext des MS-Treibers, und die Lizenznehmer von Visual Studio dürfen diesen verwenden und ihn für eigene Treiber-Entwicklungen modifizieren. Das haben die CUPS-Entwickler getan. Die Lizenz erlaubt ihnen nicht, den gesamten Quelltext zu veröffentlichen, sie haben jedoch das „*diff*“ unter der GPL veröffentlicht, und wenn Sie Besitzer eines „*MS DDK for Windows NT*“ sind, können Sie den Treiber selbst prüfen.

18.9 Das Konfigurieren von CUPS für den Download von Treibern

Wie wir zuvor erwähnt haben, funktionieren alle bekannten Methoden, um Client-Drucker-Treiber auf dem Samba-Server vorzubereiten (und damit die Vorzüge von Point'n'Print zu genießen), auch mit CUPS. Diese Methoden wurden im vorigen Kapitel beschrieben. In Wirklichkeit ist dies eine reine Samba-Angelegenheit und hängt nur mit dem Verhältnis Samba/Windows-Client zusammen.

18.9.1 *cupsaddsmb*: Das unbekannte Hilfsmittel

Das Werkzeug **cupsaddsmb** (das mit allen aktuellen CUPS-Versionen ausgeliefert wird) ist eine alternative Methode, um Druckertreiber in die Samba-Freigabe *[print$]* zu transferieren. Zur Erinnerung: Diese Freigabe ist der Ort, an dem Clients nach hinterlegten und konfigurierten Treibern suchen, um diese herunterzuladen und zu installieren. Dies macht das Verteilen von jeglichen (oder allen) installierten CUPS-Druckern ziemlich einfach. **cupsaddsmb** kann den Adobe PostScript-Treiber genauso verwenden wie den neu entwickelten CUPS-PostScript-Treiber für Windows NT/200x/XP. *cupsaddsmb* funktioniert *NICHT* mit beliebigen Druckertreibern, sondern nur mit *exakt* den Treiber-Dateien, die in seiner Manpage angegeben sind.

Der CUPS-Druckertreiber ist auf der CUPS-Download-Seite verfügbar. Sein Paketname ist `cups-samba-[version].tar.gz`. Er wird den Adobe-Treibern vorgezogen, da er einige Vorteile hat:

- Er unterstützt eine genauere Seiten-Abrechnung.
- Er unterstützt Banner-Seiten und Seiten-Labels auf allen Druckern.
- Er unterstützt das Setzen von einigen IPP-Auftragsattributen (wie Auftragspriorität, Seiten-Label und Auftragsverrechnung).

Derzeit werden jedoch nur Windows NT, 2000 und XP von den CUPS-Treibern unterstützt. Sie brauchen auch die entsprechenden Teile des Adobe-Treibers, wenn Sie Windows 95-, 98- und ME-Clients unterstützen müssen.

18.9.2 Bereiten Sie Ihre smb.conf für cupsaddsmb vor

Vor dem Ausführen von **cupsaddsmb** müssen Sie die Einstellungen in `smb.conf` wie im nächsten Beispiel setzen:

18.9.3 CUPS „*PostScript-Treiber für Windows NT/200x/XP*“

CUPS-Anwender können die genau gleichen Pakete von <`http://www.cups.org/software.html`> beziehen. Dies ist ein separates Paket von CUPS-Software-Dateien, das als „*CUPS 5.0rc3 Windows NT/200x/XP Printer Driver for Samba*“ bezeichnet wird. Der Dateiname für den Download ist `cups-samba-5.0rc3.tar.gz`. Nach dem untar und unzip zeigen sich folgende Dateien:

```
root# tar xvzf cups-samba-5.0rc3.tar.gz
cups-samba.install
cups-samba.license
cups-samba.readme
cups-samba.remove
cups-samba.ss
```

Diese Dateien wurden mit der ESP-Meta-Packer-Software EPM gepackt. Die Dateien `*.install` und `*.remove` sind einfache Shell-Skripten, die die Datei `*.ss` entpacken (die

Beispiel 18.9.1. smb.conf für die Verwendung von cupsaddsmb

```
[global]
       load printers = yes
       printing = cups
       printcap name = cups

[printers]
       comment = Alle Drucker
       path = /var/spool/samba
       browseable = no
       public = yes
# Einstellung ist abhängig von Ihren Anforderungen
       guest ok = yes
       writable = no
       printable = yes
       printer admin = root

[print$]
       comment = Druckertreiber
       path = /etc/samba/drivers
       browseable = yes
       guest ok = no
       read only = yes
       write list = root
```

Datei `*.ss` ist nichts als ein tar-Archiv, das auch mit „*tar*“ entpackt werden kann). Dann kopiert sie deren Inhalt in `/usr/share/cups/drivers/`. Dieser Inhalt enthält drei Dateien:

```
root# tar tv cups-samba.ss
cupsdrvr.dll
cupsui.dll
cups.hlp
```

Das Shell-Skript *cups-samba.install* ist einfach anzuwenden:

```
root# ./cups-samba.install
[....]
Installing software...
Updating file permissions...
Running post-install commands...
Installation is complete.
```

Das Skript sollte die Treiber-Dateien automatisch ins Verzeichnis `/usr/share/cups/drivers/` kopieren.

> **Warnung**
>
> Wegen eines Fehlers kopiert eine ältere CUPS-Release die Datei `cups.hlp` ins Verzeichnis `/usr/share/drivers/` statt in `/usr/share/cups/drivers/`. Um dieses Problem zu beheben, kopieren/verschieben Sie diese Datei einfach manuell ins richtige Verzeichnis, nachdem Sie das Install-Skript ausgeführt haben.

```
root# cp /usr/share/drivers/cups.hlp /usr/share/cups/drivers/
```

Dieser neue CUPS-PostScript-Treiber ist derzeit nur binär verfügbar, ist aber kostenlos. Es wird (noch) kein vollständiger Quelltext zur Verfügung gestellt. Der Grund ist, dass er mit Hilfe des Microsoft Driver Developer Kits (DDK) entwickelt und mit Microsoft Visual Studio 6 kompiliert wurde. Die Treiber-Entwickler dürfen nicht den gesamten Quelltext als freie Software vertreiben. Die CUPS-Entwickler haben jedoch das „*diff*“ unter der GPL veröffentlicht, somit kann jeder mit einer Lizenz für Visual Studio und einem DDK den Treiber selbst kompilieren.

18.9.4 Das Erkennen verschiedener Treiber-Dateien

Die CUPS-Treiber unterstützen die älteren Systeme Windows 95/98/Me nicht, nur die Client-Systeme Windows NT/2000/XP.

Windows NT, 2000 und XP werden unterstützt von:

- cups.hlp
- cupsdrvr.dll
- cupsui.dll

Adobe-Treiber sind für die älteren Systeme Windows 95/98/Me genauso verfügbar wie für Windows NT/2000/XP. Die Dateien sind für die einzelnen Plattformen verschieden.

Windows 95, 98 und ME werden unterstützt von:

- ADFONTS.MFM
- ADOBEPS4.DRV
- ADOBEPS4.HLP
- DEFPRTR2.PPD
- ICONLIB.DLL

- PSMON.DLL

Windows NT, 2000 und XP werden unterstützt von:

- ADOBEPS5.DLL
- ADOBEPSU.DLL
- ADOBEPSU.HLP

ANMERKUNG

Wenn sowohl die Adobe-Treiber-Dateien als auch die CUPS-Treiber-Dateien zur Unterstützung von Windows NT/200x/XP vorhanden sind, werden die Adobe-Dateien ignoriert und die CUPS-Dateien verwendet. Wenn Sie — aus irgendeinem Grund— nur Adobe-Treiber verwenden wollen, entfernen Sie einfach die drei CUPS-Dateien. Windows 9x/Me-Clients verwenden in jedem Fall die Adobe-Treiber.

18.9.5 Das Beschaffen der Adobe-Treiber-Dateien

Das Beschaffen der Adobe-Treiber-Dateien scheint für viele Anwender unerwartet schwierig zu sein. Sie sind nicht als einzelne Dateien auf der Adobe-Website erhältlich, und die selbstentpackende und/oder selbstinstallierende Windows-.exe-Datei ist auch nicht einfach zu finden. Möglicherweise müssen Sie den enthaltenen Installer verwenden und die Installation einmal auf einem Client durchführen. Dies installiert die Treiber (und einen generischen PostScript-Drucker) lokal auf dem Client. Wenn diese installiert sind, geben Sie den generischen PostScript-Drucker frei. Danach enthält die Freigabe *[print$]* des Clients die Adobe-Dateien, von wo aus Sie sie mittels smbclient auf den CUPS-Host holen können.

18.9.6 ESP Print Pro PostScript-Treiber für Windows NT/200x/XP

Die Anwender der Software ESP Print Pro können ihr Samba-Treiber-Paket für diesen Zweck ohne Probleme installieren. Beziehen Sie die Treiber-Dateien aus dem normalen Download-Bereich der ESP Print Pro-Software unter <`http://www.easysw.com/software.html`>. Sie müssen den Link namens „*SAMBA*“ unter **Download Printer Drivers for ESP Print Pro 4.x** finden und das Package herunterladen. Sobald es instaliert ist, können Sie jeden Treiber vorbereiten, indem Sie einfach den Drucker im Drucker-Manager-GUI markieren und die Funktion **Export Driver...** aus dem Menü wählen. Natürlich müssen Sie Samba zuerst für den Umgang mit den Treiber-Dateien vorbereitet haben, also die Freigabe *[print$]* angelegt haben und so weiter. Das Paket ESP Print Pro beinhaltet die CUPS-Treiber-Dateien genauso wie ein (lizenziertes) Set von Adobe-Treibern für die Windows 95/98/Me-Client-Familie.

18.9.7 Vorbehalte(((Fallstricke ?))), die zu berücksichtigen sind

Sobald Sie das Install-Skript ausgeführt haben (und eventuell die Datei `cups.hlp` manuell nach `/usr/share/cups/drivers/` verschoben haben), kann der Treiber in die Samba-Freigabe *[print$]* gelegt werden (die oft auf das Verzeichnis `/etc/samba/drivers/` zeigt und einen Unterverzeichnis-Baum mit den Verzeichnissen *WIN40* und *W32X86* enthält). Sie tun dies, indem Sie **cupsaddsmb** ausführen (sehen Sie dazu auch **man cupsaddsmb**, für alle CUPS-Releases seit 1.1.16).

TIPP

Es kann sein, dass Sie root in die Datei `smbpasswd` aufnehmen müssen, indem Sie **smbpasswd** ausführen; dies ist besonders wichtig, wenn Sie diese ganze Prozedur zum ersten Mal ausführen und nicht in einer Umgebung arbeiten, in der alles für *Single Sign On* an einem Windows-Domänencontroller konfiguriert ist.

Sobald die Treiber-Dateien in der Freigabe *[print$]* liegen und initialisiert sind, können sie von den Windows NT/200x/XP Clients heruntergeladen und installiert werden.

ANMERKUNG

Win 9x/Me-Clients funktionieren nicht mit dem CUPS-PostScript-Treiber. Für diese Clients brauchen Sie nach wie vor die `ADOBE*.*`-Treiber, wie oben erwähnt.

ANMERKUNG

Es macht nichts, wenn Sie immer noch die `ADOBE*.*`-Treiber-Dateien aus älteren Installationen im Verzeichnis `/usr/share/cups/drivers/` liegen haben. Das neue **cupsaddsmb** (ab 1.1.16) bevorzugt automatisch die eigenen Treiber, wenn es beide vorfindet.

ANMERKUNG

Sollten Ihre Windows-Clients die alten `ADOBE*.*`-Treiber-Dateien installiert haben, wird der Download des neuen CUPS-PostScript-Treibers zuerst scheitern. Sie müssen den alten Treiber zuerst von den Clients löschen. Es reicht nicht aus, den Drucker zu „*löschen*“, da die Treiber-Dateien nach wie vor von den Clients bereitgestellt und wiederverwendet werden, wenn Sie versuchen, den Drucker neu zu installieren. Um die Adobe-Treiber auf den Clients völlig loszuwerden, öffnen Sie den Ordner **Drucker** (evtl. via **Start** > **Systemsteuerung** > **Drucker und Faxgeräte**), klicken mit der rechten Maustaste auf den Ordner-Hintergrund und wählen **Servereigenschaften**. Wenn sich der neue Dialog öffnet, wählen Sie den Reiter **Treiber**. In der Liste wählen Sie den Treiber, den Sie löschen wollen, und klicken auf **Entfernen**. Dies funktioniert nur, wenn kein einziger Drucker mehr übrig ist, der diesen Treiber verwendet. Sie müssen zuerst alle Drucker im Ordner **Drucker** „*löschen*“, die diesen Treiber verwenden. Sie brauchen Administrator-Rechte, um dies zu tun.

ANMERKUNG

Sobald Sie erfolgreich den CUPS-PostScript-Treiber auf einen Client geladen haben, können Sie leicht alle Drucker auf diesen Treiber umstellen, indem Sie so vorgehen, wie im Abschnitt Classical Printing Support beschrieben. Entweder ändern Sie den Treiber für einen vorhandenen Drucker, indem Sie den Dialog **Drucker-Eigenschaften** verwenden, oder Sie benutzen den Befehl **rpcclient** mit der Option **setdriver**.

18.9.8 Windows CUPS-PostScript-Treiber versus Adobe-Treiber

Interessiert Sie ein Vergleich des CUPS- und des Adobe-Treibers? Für unsere Zwecke sind dies die wichtigsten Punkte, die für den CUPS-Treiber sprechen:

- Es gibt keine Probleme mit der Adobe-EULA.
- es gibt keine Probleme mit der Frage „*Wo kriege ich die Adobe-Treiber-Dateien her?*“
- Die Adobe-Treiber fügen (auf Anfrage der zugeordneten PPD-Datei) oft einen PJL-Header vor dem Haupt-PS-Teil der Druck-Datei ein. Daher beginnt die Druck-Datei mit *<1B >%-12345X* oder *<escape>%-12345X* anstatt mit *%!PS*. Das führt dazu, dass der CUPS-Daemon die eintreffende Datei automatisch als druckfertig kennzeichnet und sie nicht durch den Filter *pstops* schickt (technisch ausgedrückt, wird die Datei nicht als der generische MIME-Typ *application/postscript*, sondern als MIME-

Typ *application/cups.vnd-postscript* eingestuft). Das führt auch dazu, dass die Seitenzählung in */var/log/cups/page_log* nicht die exakte Seitenanzahl erhält; stattdessen wird die Dummy-Seitenzahl „*1*“ in einem Standard-Setup protokolliert.

- Der Adobe-Treiber hat mehr Optionen, um das von ihm generierte PostScript falsch zu konfigurieren (z.B. kann er es versehentlich auf **Optimize for Speed** anstatt auf **Optimize for Portability** setzen, was dazu führen kann, dass CUPS es nicht mehr verarbeiten kann).
- Die Ausgabe des CUPS-PostScript-Treibers, die von Windows-Clients an den CUPS-Server gesendet wird, wird garantiert als generischer MIME-Typ *application/postscript* typisiert und daher auch zuverlässig durch den Filter *pstops* geschickt, was für Abrechnungs- und Quota-Zwecke die korrekte Seitenzahl in `page_log` ergibt.
- Der CUPS-PostScript-Treiber unterstützt das Senden von zusätzlichen Standard-Druckoptionen (IPP) durch Windows NT/200x/XP-Clients. Solche zusätzlichen Druckoptionen sind: das Benennen der Standard-CUPS-*Banner-Seiten* (oder der benutzerdefinierten, sollten sie zum Zeitpunkt des Treiber-Downloads installiert sein) unter Verwendung der CUPS-Option page-label, das Setzen einer Auftragspriorität und das Setzen einer Ausführungszeit des Drucks (mit der Option, dass zukünftig noch weitere IPP-Auftragsattribute unterstützt werden).
- Der CUPS-PostScript-Treiber unterstützt das Einschließen von neuen **cupsJobTicket*-Parametern am Anfang der PostScript-Datei (die in Zukunft für alle möglichen nützlichen Erweiterungen auf CUPS-Seite verwendet werden können, aber keinerlei andere Anwendungen stören werden, da diese sie einfach als Kommentar betrachten und ignorieren werden).
- Der CUPS-PostScript-Treiber wird das Herzstück des voll ausgewachsenen CUPS-IPP-Clients für Windows NT/200x/XP sein, der bald veröffentlicht werden soll (möglicherweise parallel zur ersten Beta-Release von CUPS 1.2).

18.9.9 Das Ausführen von cupsaddsmb (im Quiet Mode)

Der Befehl **cupsaddsmb** kopiert die benötigten Dateien in Ihre Freigabe *[print$]*. Zusätzlich wird das mit dem Drucker assoziierte PPD von `/etc/cups/ppd/` in *[print$]* kopiert. Dort warten diese Dateien auf praktische Windows-Client-Installationen via Point'n'Print. Bevor wir den Befehl erfolgreich ausführen können, müssen wir sicher sein, dass wir uns am Samba-Server authentifizieren können. Wenn Sie ein kleines Netzwerk haben, verwenden Sie möglicherweise User-level-Sicherheit (security = user).

Hier ein Beispiel für ein erfolgreich ausgeführtes **cupsaddsmb**:

```
root# cupsaddsmb -U root infotec_IS2027
Password for root required to access localhost via Samba: ['secret']
```

Um *alle* Drucker und Treiber freizugeben, verwenden Sie den Parameter `-a` anstatt des Drucker-Namens. Da **cupsaddsmb** die Druckertreiber an Samba „*exportiert*“, sollte es

[] C: $netuselpt1 : sambaserver/user : ntadmin$

Führen Sie rpcclient setdriver aus.

Configfile: [C:3232X86“2.DLL] Helpfile: [C:3232X86“2.HLP] Dependentfiles: [] Dependentfiles: [] Dependentfiles: [] Dependentfiles: [] Dependentfiles: [] Dependentfiles: [] Monitorname: [] Defaultdatatype: []

(Optional) Prüfen, ob der Drucker von Samba erkannt wird. [] root rpcclient -Uroot— grep -C2 mysmbtstprn flags:[0x800000] name:[kde-bitshop] description:[kde-bitshop,,mysmbtstprn] comment:[mysmbtstprn]

(((Ab hier erscheint der Rest des Abschnitts in der PDF-Datei in Kapit“344lchen.))) Dies installiert den Drucker mit dem Namen mysmbtstprn im CUPS-System. Der Drucker wird “374ber eine Socket-Verbindung (auch als JetDirect oder Direct TCP/IP bekannt) angesprochen. Sie m“374ssen f“374r diesen Schritt root sein.

Dies sollte den Drucker in der Liste anzeigen. Wenn nicht, stoppen Sie den Samba-Daemon (smbd), und starten Sie ihn neu, oder senden Sie ein HUP-Signal: []

root kill -HUP ‘pidof smbd‘

Pr“374fen Sie nochmals. Korrigieren Sie, und wiederholen Sie dies, bis zum Erfolg. Beachten Sie das “214leere“215 Feld zwischen den beiden Kommas in der Zeile “214description“215. Der Treibername w“374rde hier erscheinen, wenn es bereits einen g“344be. Sie m“374ssen das Samba-Passwort von root kennen (wie es vom Befehl smbpasswd gesetzt wurde), um diesen Schritt und die meisten der folgenden Schritte ausf“374hren zu k“366nnen. Alternativ dazu k“366nnen Sie sich als einer der Benutzer authentifizieren, die in der “214write list“215 f“374r [print“044] in smb.conf definiert sind.

(Optional) Prüfen, ob Samba einen Treiber für den Drucker kennt. []

root rpcclient -Uroot— grep driver

drivername:[]

root rpcclient -Uroot— grep -C4 driv

servername:[kde-bitshop]

printername:[kde-bitshop]

sharename:[mysmbtstprn]

portname:[Samba Printer Port]

drivername:[]

comment:[mysmbtstprn]

location:[]

sepfile:[]

printprocessor:[winprint]

root rpcclient -U rootresult was $\mathrm{WERR}_{UNKNOWN_{PRINTER_{DRIVER}}}$

Keiner der drei oben gezeigten Befehle sollte einen Treiber anzeigen. Dieser Schritt wurde nur ausgeführt, um diese Bedingung zu demonstrieren. Ein Versuch, sich in diesem Stadium mit dem Drucker zu verbinden, sollte folgende Nachricht zeigen: „*Der Server hat nicht die erforderlichen Treiber installiert.*“

Stellen Sie alle erforderlichen Treiberdateien in die Samba-Freigabe [print$].

```
root# smbclient //localhost/print\$ -U 'root%xxxx' \
   -c 'cd W32X86; \
   put /etc/cups/ppd/mysmbtstprn.ppd mysmbtstprn.PPD; \
   put /usr/share/cups/drivers/cupsui.dll cupsui.dll; \
```

```
   put /usr/share/cups/drivers/cupsdrvr.dll cupsdrvr.dll; \
   put /usr/share/cups/drivers/cups.hlp cups.hlp'
```

(Dieser Befehl sollte in einer einzelnen langen Zeile eingegeben werden; die durch „\“ angezeigten Zeilenumbrüche wurden nur eingefügt, um die Lesbarkeit zu verbessern. Dieser Schritt ist *erforderlich*, damit der darauf folgende Schritt erfolgreich durchgeführt werden kann. Er macht die Dateien physisch in der Freigabe *[print$]* verfügbar. Die Clients wären jedoch nach wie vor nicht in der Lage, diese Treiber zu installieren, da Samba sie noch nicht als Treiberdateien behandelt. Ein Client, der diesen Treiber abfragt, würde nach wie vor mit einer Meldung wie „*nicht installiert*“ konfrontiert.

Prüfen, wo sich die Treiberdateien jetzt befinden.

```
root# ls -l /etc/samba/drivers/W32X86/
total 669
drwxr-sr-x    2 root     ntadmin       532 May 25 23:08 2
drwxr-sr-x    2 root     ntadmin       670 May 16 03:15 3
-rwxr--r--    1 root     ntadmin     14234 May 25 23:21 cups.hlp
-rwxr--r--    1 root     ntadmin    278380 May 25 23:21 cupsdrvr.dll
-rwxr--r--    1 root     ntadmin    215848 May 25 23:21 cupsui.dll
-rwxr--r--    1 root     ntadmin    169458 May 25 23:21 mysmbtstprn.PPD
```

Die Treiberdateien sind jetzt im „*Wurzelverzeichnis*“ der Freigabe *[print$]*.

Samba mitteilen, dass diese Dateien Treiberdateien sind (adddriver).

```
root# rpcclient -Uroot%xxxx -c 'adddriver "Windows NT x86" \
   "mydrivername:cupsdrvr.dll:mysmbtstprn.PPD: \
  cupsui.dll:cups.hlp:NULL:RAW:NULL"' \
  localhost
Printer Driver mydrivername successfully installed.
```

Sie können diesen Schritt nicht wiederholen, wenn er scheitert. Er könnte sogar infolge eines simplen Tippfehlers scheitern. Meist hat der Befehl dann bereits einen Teil der Treiberdateien in das Unterverzeichnis „*2*“ verschoben. Wenn dieser Schritt scheitert, müssen Sie zum vierten Schritt zurückgehen und ihn wiederholen, bevor Sie den fünften Schritt von neuem versuchen können. In diesem Schritt müssen Sie einen Namen für Ihren Treiber auswählen. Es ist normalerweise eine gute Idee, denselben Namen zu verwenden, wie er für den Druckernamen verwendet wird; in großen Installationen werden Sie jedoch diesen Treiber für eine größere Anzahl von Druckern verwenden, die natürlich verschiedene Namen haben, daher ist der Name des Treibers nicht fixiert.

Prüfen, wo sich die Treiberdateien jetzt befinden.

```
root# ls -l /etc/samba/drivers/W32X86/
total 1
```

```
drwxr-sr-x    2 root     ntadmin       532 May 25 23:22 2
drwxr-sr-x    2 root     ntadmin       670 May 16 03:15 3

root# ls -l /etc/samba/drivers/W32X86/2
total 5039
[....]
-rwxr--r--    1 root     ntadmin     14234 May 25 23:21 cups.hlp
-rwxr--r--    1 root     ntadmin    278380 May 13 13:53 cupsdrvr.dll
-rwxr--r--    1 root     ntadmin    215848 May 13 13:53 cupsui.dll
-rwxr--r--    1 root     ntadmin    169458 May 25 23:21 mysmbtstprn.PPD
```

Beachten Sie, wie der Schritt 6 auch die Treiberdateien in das entsprechende Unterverzeichnis verschoben hat. Vergleichen Sie dies mit der Situation nach dem Schritt 5.

(Optional) Prüfen, ob Samba jetzt den Treiber erkennt.

```
root# rpcclient -Uroot%xxxx -c 'enumdrivers 3' \
   localhost | grep -B2 -A5 mydrivername
Printer Driver Info 3:
Version: [2]
Driver Name: [mydrivername]
Architecture: [Windows NT x86]
Driver Path: [\\kde-bitshop\print$\W32X86\2\cupsdrvr.dll]
Datafile: [\\kde-bitshop\print$\W32X86\2\mysmbtstprn.PPD]
Configfile: [\\kde-bitshop\print$\W32X86\2\cupsui.dll]
Helpfile: [\\kde-bitshop\print$\W32X86\2\cups.hlp]
```

Erinnern Sie sich: Dieser Befehl führt ein „*grep*“ nach dem Namen aus, den Sie im Schritt 6 für den Treiber gewählt haben. Dieser Befehl muss erfolgreich ausgeführt worden sein, bevor Sie fortfahren können.

Samba mitteilen, welcher Drucker diese Treiberdateien verwenden soll (**setdriver**).

```
root# rpcclient -Uroot%xxxx -c 'setdriver mysmbtstprn mydrivername' \
   localhost
Successfully set mysmbtstprn to driver mydrivername
```

Da Sie jeden Druckernamen (Drucker-Queue) an jeden Treiber binden können, ist dies eine praktische Möglichkeit, viele Queues zu konfigurieren, die denselben Treiber verwenden. Sie brauchen all die vorhergehenden Schritte nicht zu wiederholen, damit der Befehl **setdriver** Erfolg hat. Die einzigen Vorbedingungen sind: **enumdrivers** muss den Treiber finden, und **enumprinters** muss den Drucker finden.

(Optional) Prüfen, ob Samba diese Zuordnung erkannt hat.

```
root# rpcclient -Uroot%xxxx -c 'getprinter mysmbtstprn 2' localhost \
```

```
  | grep driver
drivername:[mydrivername]

root# rpcclient -Uroot%xxxx -c 'getprinter mysmbtstprn 2' localhost \
  | grep -C4 driv
servername:[\\kde-bitshop]
printername:[\\kde-bitshop\mysmbtstprn]
sharename:[mysmbtstprn]
portname:[Done]
drivername:[mydrivername]
comment:[mysmbtstprn]
location:[]
sepfile:[]
printprocessor:[winprint]

root# rpcclient -U root%xxxx -c 'getdriver mysmbtstprn' localhost
[Windows NT x86]
Printer Driver Info 3:
     Version: [2]
     Driver Name: [mydrivername]
     Architecture: [Windows NT x86]
     Driver Path: [\\kde-bitshop\print$\W32X86\2\cupsdrvr.dll]
     Datafile: [\\kde-bitshop\print$\W32X86\2\mysmbtstprn.PPD]
     Configfile: [\\kde-bitshop\print$\W32X86\2\cupsui.dll]
     Helpfile: [\\kde-bitshop\print$\W32X86\2\cups.hlp]
     Monitorname: []
     Defaultdatatype: [RAW]
     Monitorname: []
     Defaultdatatype: [RAW]

root# rpcclient -Uroot%xxxx -c 'enumprinters' localhost \
   | grep mysmbtstprn
     name:[\\kde-bitshop\mysmbtstprn]
     description:[\\kde-bitshop\mysmbtstprn,mydrivername,mysmbtstprn]
     comment:[mysmbtstprn]
```

Vergleichen Sie diese Resultate mit denen aus den Schritten 2 und 3. Jeder dieser Befehle zeigt, dass der Treiber installiert ist. Sogar der Befehl **enumprinters** führt jetzt den Treiber in der Zeile „*description*“ an.

(Optional) Den Treiber in den korrekten Gerätemodus „*kitzeln*“. Sie wissen sicherlich, wie man den Treiber auf dem Client installiert. Für den Fall, dass Sie nicht besonders vertraut mit Windows sind, hier ein Schnell-Rezept: Durchsuchen Sie die Netzwerkumgebung, gehen Sie auf den Samba-Server, und sehen Sie nach den Freigaben. Sie sollten hier alle freigegebenen Samba-Drucker sehen. Klicken Sie doppelt auf den gewünschten Drucker. Der Treiber sollte installiert und die Netzwerkverbindung hergestellt werden. Eine weitere Möglichkeit ist, den Ordner **Drucker und Faxgeräte** zu öffnen, den betreffenden Drucker

mit der rechten Maustaste anzuklicken und entweder **Verbinden** oder **Installieren** zu wählen. Als Ergebnis sollte ein neuer Drucker in dem lokalen Ordner **Drucker und Faxgeräte** Ihres Clients erscheinen, der **Druckerfreigabename auf SambaServerName** oder so ähnlich heißt. Es ist wichtig, dass Sie diesen Schritt als ein Samba-Drucker-Administrator (printer admin, definiert in `smb.conf`) ausführen. Hier eine andere Methode, dies in Windows XP zu tun. Diese Methode verwendet eine Befehlszeile, die Sie in der „*DOS box*“ eingeben (tippen Sie das smbpassword von root, falls erforderlich):

```
C:\> runas /netonly /user:root "rundll32 printui.dll,PrintUIEntry \
   /in /n \\sambaserver\mysmbtstprn"
```

Ändern Sie irgendeine Druckereinstellung einmal (wie z.B. den Parameter **portrait** *auf* **landscape**), klicken Sie auf **Übernehmen**,und ändern Sie die Einstellung wieder zurück.

Den Drucker auf einem Client installieren (Point'n'Print).

```
C:\> rundll32 printui.dll,PrintUIEntry /in /n \\sambaserver\mysmbtstprn
```

Wenn dies nicht funktioniert, könnte dies ein Berechtigungsproblem mit der Freigabe *[print$]* sein.

(Optional) Eine Testseite drucken.

```
C:\> rundll32 printui.dll,PrintUIEntry /p /n "\\sambaserver\mysmbtstprn"
```

Drücken Sie fünfmal [TAB], zweimal [ENTER], einmal [TAB] und nochmals [ENTER], und marschieren Sie zum Drucker.

(Empfohlen) Studieren Sie die Testseite. Hmmm.... ich scherze nur! Mittlerweile wissen Sie alles über Drucker-Installationen und brauchen kein Wort mehr davon zu lesen. Stecken Sie die Seite in einen Rahmen, und nageln Sie den an die Wand, mit der Überschrift MEIN ERSTER MIT RPCCLIENT INSTALLIERTER DRUCKER– oder werfen Sie sie einfach weg!

(Obligatorisch) Genießen Sie es. Machen Sie Luftsprünge. Feiern Sie Ihren Erfolg.

```
root# echo "Cheeeeerioooooo! Erfolg ..." >> /var/log/samba/log.smbd
```

18.9.11 Wiedersehen mit dem Troubleshooting

Der Befehl **setdriver** wird scheitern, wenn in Sambas „*Bewusstsein*“ die Queue noch nicht vorhanden ist. Sie hatten viel versprechende Meldungen wie

```
Printer Driver ABC successfully installed.
```

nach dem Abschnitt mit **adddriver**? Aber Sie sehen auch eine enttäuschende Meldung wie diese hier?

```
result was NT_STATUS_UNSUCCESSFUL
```

Es reicht nicht aus, dass Sie mit dem Befehl **lpstat -p ir85wm** die Queue in CUPS sehen können. Ein Bug in den neueren Versionen von Samba verhindert ein ordnungsgemäßes Update der Queue-Liste. Die Erkennung von neu installierten CUPS-Druckern scheitert, bis Sie Samba neu starten oder ein HUP an alle smbd-Prozesse senden. Um zu prüfen, ob dies der Grund dafür ist, dass Samba den Befehl **setdriver** nicht erfolgreich ausführt, prüfen Sie, ob Samba den Drucker „*sieht*“:

```
root# rpcclient transmeta -N -U'root%xxxx' -c 'enumprinters 0'|grep ir85wm
        printername:[ir85wm]
```

Ein anderer Befehl könnte der hier sein:

```
root# rpcclient transmeta -N -U'root%secret' -c 'getprinter ir85wm'
        cmd = getprinter ir85wm
        flags:[0x800000]
        name:[\\transmeta\ir85wm]
        description:[\\transmeta\ir85wm,ir85wm,DPD]
        comment:[CUPS PostScript-Treiber for Windows NT/200x/XP]
```

Übrigens, Sie können diese Befehle (sowie einige weitere) natürlich auch dazu verwenden, Treiber auf entfernten Windows-NT-Druckservern zu installieren!

18.10 Die *.tdb-Dateien für das Drucken

Einige Mysterien ranken sich um die Gruppe der Dateien mit dem Suffix tdb, die in jeder Samba-Installation auftauchen. Diese sind `connections.tdb`, `printing.tdb`, `share_info.tdb`, `ntdrivers.tdb`, `unexpected.tdb`, `brlock.tdb`, `locking.tdb`, `ntforms.tdb`, `messages.tdb` , `ntprinters.tdb`, `sessionid.tdb` und `secrets.tdb`. Was ist ihr Zweck?

18.10.1 Triviale Datenbank-Dateien

Ein Windows NT-(Druck-)Server führt Buch über alle benötigten Informationen, die er zur Erfüllung seiner Pflichten gegenüber den Clients benötigt, indem er Einträge in der Windows-Registrierung speichert. Client-Anfragen werden beantwortet, indem aus der Registrierung gelesen wird, und Administrator- oder Benutzer-Konfigurationseinstellungen

werden gespeichert, indem in die Registrierung geschrieben wird. Samba und UNIX haben natürlich keine solche Registrierung. Samba führt stattdessen Buch über alle clientbezogenen Informationen, indem es eine Reihe von `*.tdb`-Dateien verwendet. (TDB = Trivial Data Base). Diese sind oft in `/var/lib/samba/` oder `/var/lock/samba/` abgelegt. Die druck-bezogenen Dateien sind `ntprinters.tdb`, `printing.tdb`, `ntforms.tdb` und `ntdrivers.tdb`.

18.10.2 Binär-Format

`*.tdb`-Dateien sind nicht für den Menschen lesbar. Sie sind in einem binären Format geschrieben. „*Warum nicht in ASCII?*“, könnten Sie fragen. „*ASCII-Dateien sind doch eine gute und bewährte Tradition unter UNIX.*“ Der Grund für diese Design-Entscheidung ist hauptsächlich die Performance. Samba muss schnell laufen; es führt für jede Client-Verbindung einen separaten **smbd**-Prozess aus, in manchen Umgebungen viele Tausende davon. Manche smbds könnten Schreibzugriff auf dieselbe `*.tdb`-Datei *zur gleichen Zeit* brauchen. Das Dateiformat der `*.tdb`-Dateien von Samba erlaubt dies; viele smbd-Prozesse können gleichzeitig in dieselbe `*.tdb`-Datei schreiben. Dies wäre mit reinen ASCII-Dateien nicht möglich.

18.10.3 *.tdb-Dateien verlieren

Es ist sehr wichtig, dass alle `*.tdb`-Dateien über alle Lese- und Schreibzugriffe hinweg konsistent bleiben. Es kann jedoch passieren, dass diese Dateien beschädigt *werden*. (Ein **kill -9 ‘pidof smbd’** während eines Schreibzugriffs könnte genauso gut dafür verantwortlich sein wie ein Stromausfall etc.). Im Falle von Schwierigkeiten kann das Löschen der alten druckbezogenen `*.tdb`-Dateien die einzige Möglichkeit sein. Danach müssen Sie alle druckbezogenen Einstellungen wieder herstellen, oder Sie haben rechtzeitig ein Backup der relevanten Dateien erstellt.

18.10.4 Das Verwenden von tdbbackup

Samba enthält ein kleines Hilfsmittel, das dem root-Benutzer Ihres Systems hilft, die `*.tdb`-Dateien zu sichern. Wenn Sie es ohne Argumente ausführen, gibt es Auskunft über seine Verwendung:

```
root# tdbbackup
 Usage: tdbbackup [options] <fname...>

 Version:3.0a
   -h            this help message
   -s suffix     set the backup suffix
   -v            verify mode (restore if corrupt)
```

Hier sehen Sie, wie ich meine Datei `printing.tdb` gesichert habe:

```
root# ls
.               browse.dat     locking.tdb     ntdrivers.tdb printing.tdb
..              share_info.tdb connections.tdb messages.tdb  ntforms.tdb
printing.tdbkp unexpected.tdb brlock.tdb      gmon.out      namelist.debug
ntprinters.tdb sessionid.tdb

root# tdbbackup -s .bak printing.tdb
 printing.tdb : 135 records

root# ls -l printing.tdb*
 -rw-------    1 root     root        40960 May  2 03:44 printing.tdb
 -rw-------    1 root     root        40960 May  2 03:44 printing.tdb.bak
```

18.11 CUPS-Druckertreiber von Linuxprinting.org

CUPS besitzt eine gute Unterstützung für Drucker vom Typ HP LaserJet. Sie können den generischen Treiber wie folgt installieren:

```
root# lpadmin -p laserjet4plus -v parallel:/dev/lp0 -E -m laserjet.ppd
```

Die Option `-m` wird die Datei `laserjet.ppd` aus dem Standard-Repository für noch nicht installierte PPDs beziehen, das CUPS üblicherweise in `/usr/share/cups/model` speichert. Alternativ dazu können Sie `-P /pfad/zu/ihrer.ppd` benutzen.

Das generische `laserjet.ppd` unterstützt jedoch nicht jede spezielle Option für jedes LaserJet-kompatible Modell. Es stellt eine Art „*kleinster gemeinsamer Nenner*“ aller Modelle dar. Wenn Sie aus irgendeinem Grund für die kommerziell verfügbaren ESP Print Pro-Treiber bezahlen müssen, sollte Ihr erster Schritt darin bestehen, die Datenbank auf der Website Linuxprinting <`http://www.linuxprinting.org/printer_list.cgi`> zu befragen. Linuxprinting.org gibt exzellente Empfehlungen dazu, welcher Treiber am besten für welchen Drucker zu verwenden ist. Die dortige Datenbank wird durch die unermüdliche Arbeit von Till Kamppeter von MandrakeSoft aktuell gehalten, der auch der Hauptautor des Werkzeugs **foomatic-rip** ist.

Anmerkung

Das frühere Konzept **cupsomatic** wird nun von seinem neuen Nachfolger, dem weitaus mächtigeren **foomatic-rip**, ersetzt. **cupsomatic** wird nicht mehr weiter instand gehalten. Hier ist die neue URL zur neuen Foomatic-3.0 <`http://www.linuxprinting.org/driver_list.cgi`>-Datenbank.(((Im PDF sieht man die Web-Adresse nicht.))) Wenn Sie ein Upgrade auf **foomatic-rip** durchführen wollen, vergessen Sie nicht, auch das Upgrade auf die neuartigen PPDs für Ihre Foomatic-betriebenen Drucker durchzuführen. **foomatic-rip** arbeitet nicht mit PPDs, die für das alte **cupsomatic** generiert wurden. Die neuen PPDs entsprechen zu 100% der Adobe PPD-Spezifikation. Sie sind auch dazu gedacht, mit Samba und dem Werkzeug **cupsaddsmb** verwendet zu werden, um die Treiber für die Windows-Clients bereitzustellen!

18.11.1 Erklärungen zu foomatic-rip und Foomatic

Heutzutage verwenden die meisten Linux-Distributionen die Werkzeuge von Linuxprinting.org, um ihre druckerspezifische Software aufzubauen (die übrigens auch auf allen UNIX-Versionen und auch auf Mac OS X oder Darwin läuft). Es ist nicht so bekannt, wie es sein sollte, dass es auch ein sehr benutzerfreundliches Interface hat, das einfache Updates von Treibern und PPDs für alle unterstützten Drucker, alle Spooler, alle Betriebssysteme und alle Paketformate erlaubt (weil es keines gibt)(((?))). Seine Geschichte reicht schon einige Jahre zurück.

Erst unlängst hat Foomatic den erstaunlichen Meilenstein von 1000 gelisteten <`http://www.linuxprinting.org/printer_list.cgi?make=Anyone`> Druckermodellen geschafft. Linuxprinting.org speichert alle wichtigen Fakten über Druckertreiber und unterstützte Modelle sowie Informationen darüber, welche Optionen für die verschiedenen Treiber/Drucker-Kombinationen verfügbar sind, in seiner Foomatic <`http://www.linuxprinting.org/foomatic.html`>-Datenbank. Momentan gibt es 245 Treiber <`http://www.linuxprinting.org/driver_list.cgi`> in der Datenbank. Viele Treiber unterstützen verschiedene Modelle, und viele Modelle können mit verschiedenen Treibern betrieben werden — Sie haben die Wahl!

18.11.1.1 690 „*Perfekte*“ Drucker

Zurzeit gibt es 690 Geräte, die mit „*arbeitet perfekt*“ bezeichnet werden, 181 arbeiten größtenteils ordentlich, 96 teilweise, und 46 sind Briefbeschwerer. Wenn man bedenkt, dass die meisten dieser Drucker Nicht-PostScript-Modelle sind (PostScript-Drucker werden von CUPS automatisch perfekt unterstützt, da sie ihre eigene, vom Hersteller bereitgestellte Windows-PPD verwenden) und dass ein multi-funktionales Gerät nie als perfekt-arbeitend bezeichnet wird, solange es nicht auch unter GNU/Linux scannt und faxt und kopiert, ist dies eine wirklich erstaunliche Errungenschaft! Vor drei Jahren war die Anzahl nicht größer

als 500, und der Linux- oder UNIX-Druck war zu der Zeit nicht einmal annähernd dort, wo er jetzt ist.

18.11.1.2 Wie das Druck-HOWTO alles begründete

Vor ein paar Jahren startete Grant Taylor <`http://www2.picante.com:81/~gtaylor/`> all das. Die Wurzeln des heutigen Linuxprinting.org liegen in dem ersten Linux-Printing-HOWTO <`http://www.linuxprinting.org/foomatic2.9/howto/`>, das er verfasst hat. Als Nebenprojekt zu diesem Dokument, das vielen Linux-Anwendern und -Administratoren bei ihren ersten Schritten in diesem komplizierten und delikaten Setup half (für einen Wissenschaftler ist Drucken „*das Auftragen einer strukturierten Ablagerung von verschiedenen Mustern aus Tinten- oder Toner-Partikeln auf Papier-Substrate*“), startete er eine kleine Postgres-Datenbank mit Informationen über den Hardware- und Treiber-Zoo, aus dem das damalige Linux-Drucken bestand. Diese Datenbank wurde zur Kern-Komponente der heutigen Foomatic-Sammlung von Werkzeugen und Daten. In der Zwischenzeit wurde sie auf eine XML-Struktur umgestellt.

18.11.1.3 Foomatics seltsamer Name

„*Warum der lustige Name?*“ fragen Sie. Als es wirklich losging, im Frühling 2000, war CUPS bei weitem nicht so populär, wie es heute ist, und die meisten Systeme benutzten LPD, LPRng oder sogar PDQ. CUPS enthielt nur ein paar generische Treiber (genug für ein paar hundert verschiedene Druckermodelle). Diese unterstützten nicht so viele gerätespezifische Optionen. CUPS enthielt auch seinen eigenen eingebauten Raster-Filter (***pstoraster***, abgeleitet von Ghostscript). Auf der anderen Seite bot CUPS eine brilliante Unterstützung für das *Controlling* aller Drucker-Optionen durch standardisierte und wohldefinierte PPD-Dateien. Und CUPS war so entworfen, dass es einfach zu erweitern ist.

Taylor hatte in seiner Datenbank bereits eine beachtliche Sammlung von Fakten über viel mehr Drucker und die Ghostscript-„*Treiber*“, mit denen sie liefen. Seine Idee, PPDs aus der Datenbank-Information zu generieren und diese dazu zu benutzen, um Standard-Ghostscript-Filter in CUPS zum Funktionieren zu bringen, bewährte sich sehr gut. Sie schlug außerdem mehrere Fliegen mit einer Klappe:

- Sie machte alle aktuellen und zukünftigen Ghostscript-Filter-Entwicklungen für CUPS verfügbar.
- Sie machte eine Vielzahl von zusätzlichen Druckermodellen für CUPS-Anwender verfügbar (weil oft der traditionelle Weg über Ghostscript der einzige verfügbare war).
- Sie stellte all den Benutzern, die Ghostscript-Filter benutzen wollten (oder mussten), die vielen erweiterten Optionen von CUPS zur Verfügung (Web-Interface, GUI-Treiber-Konfiguration).

18.11.1.4 cupsomatic, pdqomatic, lpdomatic und directomatic

CUPS arbeitete mit einem schnell zusammengehackten Filter-Skript namens cupsomatic. <`http://www.linuxprinting.org/download.cgi?filename=cupsomatic&show=0`> cupsomatic schleuste die Druckdatei durch Ghostscript, wobei es automatisch den ziem-

lich komplizierten Befehl konstruierte, der dazu benötigt wurde. Es musste nur noch ins CUPS-System kopiert werden, um dieses funktionieren zu lassen. Um zu konfigurieren, wie cupsomatic den Ghostscript-Darstellungsprozess kontrolliert, ist eine CUPS-PPD erforderlich. Diese PPD wird direkt aus den Inhalten der Datenbank generiert. Für CUPS und die entsprechende Drucker/Filter-Kombination erledigte ein anderes Perl-Skript die PPD-Generierung. Nachdem das funktionierte, implementierte Taylor innerhalb weniger Tage eine ähnliche Lösung für zwei andere Spooler. Die Namen, die für diese Konfigurationsgeneratoren gewählt wurden, waren PDQ-O-Matic <http://www.linuxprinting.org/download.cgi?filename=lpdomatic&show=0> (für PDQ) und LPD-O-Matic <http://www.linuxprinting.org/download.cgi?filename=lpdomatic&show=0> (für — Sie haben es erraten — LPD); die Konfiguration verwendete hier keine PPDs, sondern andere spooler-spezifische Dateien.

Im Spätsommer jenes Jahres begann Till Kamppeter <http://www.linuxprinting.org/till/>, seine Arbeit in die Datenbank einfließen zu lassen. Kamppeter war von MandrakeSoft <http://www.mandrakesoft.com/> angestellt worden, um dessen Drucksystem auf CUPS umzustellen, nachdem die Verantwortlichen bei MadrakeSoft sein auf FLTK <http://www.fltk.org/> basierendes XPP <http://cups.sourceforge.net/xpp/> gesehen hatten (ein GUI-Frontend für den CUPS-lp-Befehl). Er fügte viele Informationen und neue Drucker hinzu, entwickelte auch die Unterstützung für andere Spooler, wie PPR <http://ppr.sourceforge.net/> (via ppromatic), GNUlpr <http://sourceforge.net/projects/lpr/> und LPRng <http://www.lprng.org/> (beide durch ein erweitertes lpdomatic), und spooler-loses Drucken (directomatic <http://www.linuxprinting.org/download.cgi?filename=directomatic&show=0>).

Also, zur Beantwortung der Frage: „*Foomatic*“ ist der allgemeine Name für all den überlappenden Code und die Daten hinter den „**omatic*“-Skripten. Foomatic brauchte bis zur Version 2.0.x (hässliche) Perl-Datenstrukturen, die an die CUPS-PPDs von Linuxprinting.org angehängt wurden. Es gab verschiedene „**omatic*“-Skripten für jeden Spooler, genauso wie verschiedene Drucker-Konfigurationsdateien.

18.11.1.5 Die *große Vereinheitlichung* ist erreicht

Dies änderte sich alles mit Foomatic 2.9 (beta) und der „*stable release*“ 3.0. Es wurde nunmehr eine Annäherung aller *omatic-Skripten erreicht, und man spricht nun von foomatic-rip. <http://www.linuxprinting.org/foomatic2.9/download.cgi?filename=foomatic-rip&show=0> Dieses einzelne Skript ist die Vereinheitlichung der davor verschiedenen spooler-spezifischen *omatic-Skripten. foomatic-rip wird von all den verschiedenen Spoolern gleicherweise benutzt, und da es PPDs lesen kann (sowohl die originalen PostScript-Drucker-PPDs als auch die von Linuxprinting.org generierten), haben plötzlich alle unterstützten Spooler die mächtigen Features der PPDs zur Verfügung. Die Benutzer brauchen nur foomatic-rip in ihr System zu stöpseln. Für die Benutzer gibt es eine erweiterte Unterstützung für Medien-Typen und -Zufuhr, und die Papiergrößen und -schächte sind einfacher zu konfigurieren.

Außerdem enthält die neue Generation der Linuxprinting.org-PPDs keine Perl-Datenstrukturen mehr. Wenn Sie der Verwalter einer Distribution sind und die vorhergehende Version von Foomatic verwendet haben, möchten Sie vielleicht die neue Version ausprobieren. Aber vergessen Sie nicht, mit der neuen Datenbank-Engine <http://www.linuxprinting.org/

download/foomatic/foomatic-db-engine-3.0.0beta1.tar.gz>einen neuen Satz von PPDs zu generieren! Privat-Anwender brauchen nur ein einzelnes neues PPD zu generieren, das spezifisch für ihren Drucker ist. Dazu befolgen Sie die Schritte <http://www.linuxprinting.org/kpfeifle/LinuxKongress2002/Tutorial/II.Foomatic-User/II.tutorial-han html>, die im Foomatic-Tutorial oder in diesem Kapitel beschrieben sind. Diese neuen Entwicklungen sind wirklich erstaunlich.

foomatic-rip ist ein sehr cleverer "Wrapperüm die Anforderung, Ghostscript mit verschiedener Syntax, verschiedenen Optionen, Geräte-Auswahl und/oder Filtern für jeden verschiedenen Drucker oder Spooler auszuführen. Zur selben Zeit kann es die PPD, die einer Drucker-Queue zugeordnet ist, lesen und den Druckauftrag entsprechend der Benutzer-Auswahl modifizieren. Dazu kommt die 100%ige Übereinstimmung der Foomatic-PPDs mit der Adobe-Spezifikation. Einige innovative Features des Foomatic-Konzepts werden die Benutzer überraschen. Es unterstützt benutzerdefinierte Papiergrößen für viele Drucker und den Druck auf Medien aus verschiedenen Schächten innerhalb desselben Auftrags (in beiden Fällen sogar dann, wenn es dafür keine Unterstützung von Windows-basierenden Hersteller-Treibern gibt).

18.11.1.6 Externe Treiberentwicklung

Der Großteil der Treiberentwicklung finden nicht innerhalb von Linuxprinting.org statt. Die Treiber werden von unabhängigen Maintainern geschrieben. Linuxprinting.org sammelt nur all die Informationen und speichert sie in seiner Datenbank. Zusätzlich stellt es den „*Leim*“ von Foomatic zur Verfügung, um die vielen Treiber in jegliches moderne (oder alte) Drucksystem zu integrieren.

Wo wir gerade von den verschiedenen Treiber-Entwickler-Gruppen sprechen, die meiste Arbeit wird derzeit in drei Projekten erledigt. Dies sind:

- Omni <http://www-124.ibm.com/developerworks/oss/linux/projects/omni/> — ein freies Software-Projekt von IBM, das versucht, das Druckertreiber-Wissen von IBM aus den guten alten OS/2-Zeiten in eine moderne, modulare, universelle Treiber-Architektur für Linux/UNIX zu konvertieren (immer noch im Beta-Stadium). Dieses Projekt unterstützt derzeit 437 Modelle.

- HPIJS <http://hpinkjet.sf.net/> — ein freies Software-Projekt von HP, um Unterstützung für die firmeneigenen Modelle anzubieten (sehr ausgereift, der Druck ist in den meisten Fällen perfekt und bietet volle Photo-Qualität). Dieses Projekt unterstützt derzeit 369 Modelle.

- Gimp-Print <http://gimp-print.sf.net/> — ein freies Software-Projekt, das von Michael Sweet (auch ein führender CUPS-Entwickler)begonnen wurde und jetzt von Robert Krawitz geleitet wird. Es hat ein erstaunliches Level von Photo-Druck-Qualität erreicht (viele Epson-Anwender schwören, dass die Qualität besser ist als die der Epson-Treiber für Microsoft-Plattformen). Dieses Projekt unterstützt derzeit 522 Modelle.

18.11.1.7 Foren, Downloads, Tutorials und HOWTOs — auch für Mac OS X und kommerzielles UNIX

Linuxprinting.org ist heute der One-Stop-Shop(((?))), um Druckertreiber herunterzuladen. Suchen Sie nach Drucker-Informationen und Tutorials <http://www.linuxprinting.org/ /kpfeifle/LinuxKongress2002/Tutorial/>, oder lösen Sie Probleme in den populären Foren. <http://www.linuxprinting.org/newsportal/> Dieses Forum ist nicht nur für GNU/Linux-Anwender, sondern auch für Admins kommerzieller UNIX-Systeme <http: //www.linuxprinting.org/macosx/>, und das ziemlich neue Mac OS X-Forum <http:// www.linuxprinting.org/newsportal/thread.php3?name=linuxprinting.macosx.general> wurde innerhalb einiger weniger Wochen zu einem der meistfrequentierten Foren.

Linuxprinting.org und die Foomatic-Treiber-Wrapper um Ghostscript sind nunmehr eine Standard-Werkzeug-Kette für das Drucken in allen wichtigen Distributionen. Die meisten haben auch CUPS darunter integriert. Während in den letzten Jahren die meisten Drucker-Daten von Kamppeter (der für Mandrake arbeitet) hinzugefügt wurden, kamen viele andere Beiträge von Leuten bei SuSE, Red Hat, Conectiva, Debian und anderen. Hersteller-Neutralität ist ein wichtiges Ziel des Foomatic-Projekts.

Anmerkung

Till Kamppeter von MandrakeSoft leistet in seiner Freizeit hervorragende Arbeit, um Linuxprinting.org und Foomatic zu pflegen. Wenn Sie diese oft nutzen, senden Sie ihm doch bitte eine kleine Mail, um Ihre Anerkennung zu zeigen.

18.11.1.8 PPDs aus der Foomatic-Datenbank

Die Foomatic-Datenbank ist selbst ein erstaunliches Stück Raffiniertheit. Sie enthält nicht nur die Drucker- und Treiber-Informationen, sondern ist auf eine Art organisiert, dass sie PPD-Dateien ad hoc aus ihren internen, auf XML basierenden Datensätzen generieren kann. Während diese PPDs der Adobe-Spezifikation für PostScript Printer Descriptions (PPDs) entsprechen, betreiben Linuxprinting.org/Foomatic-PPDs normalerweise keine PostScript-Drucker. Sie werden verwendet, um all die Features zu beschreiben, die Sie auf jedem beliebigen Gerät verwenden können. Der hauptsächliche Trick ist eine zusätzliche Zeile, die nicht von der Adobe-Spezifikation beachtet wird und mit dem Schlüsselwort **cupsFilter* beginnt. Sie teilt dem CUPS-Daemon mit, wie er mit der PostScript-Druckdatei weiter verfahren soll (ältere Foomatic-PPDs benannten das cupsomatic-Filter-Skript, während die neueren PPDs foomatic-rip aufrufen). Dieses Filter-Skript ruft Ghostscript auf dem Host-System auf (die empfohlene Variante ist ESP Ghostscript), um die erforderliche Arbeit zu tun. foomatic-rip weiß, welchen Filter oder welche interne Geräte-Einstellung es von Ghostscript verlangen muss, um den PostScript-Druckauftrag in ein Rasterformat zu wandeln, das passend für das Zielgerät ist. Diese Verwendung von PPDs, um die Optionen von Nicht-PS-Druckern zu beschreiben, war eine Erfindung der CUPS-Entwickler. Der Rest ist einfach. GUI-Werkzeuge (wie KDEs wunderbares kprinter <http://printing.kde.

org/overview/kprinter.phtml> oder gtklp <http://gtklp.sourceforge.net/> von GNOME, xpp und das CUPS-Web-Interface) lesen das PPD genauso und verwenden diese Information, um die verfügbaren Einstellungen dem Benutzer anzubieten, genauso wie eine intuitive Menü-Auswahl.

18.11.2 foomatic-rip und Foomatic-PPD-Download und -Installation

Hier sind die erforderlichen Schritte, um einen von foomatic-rip betriebenen LaserJet 4 Plus-kompatiblen Drucker in CUPS zu installieren. (Beachten Sie, dass aktuelle Distributionen von SuSE, UnitedLinux und Mandrake möglicherweise mit einem kompletten Package von Foomatic-PPDs geliefert werden, plus dem Werkzeug **foomatic-rip**. Der Besuch von Linuxprinting.org stellt sicher, dass Sie die aktuellsten Treiber und PPD-Dateien haben.)

- Öffnen Sie Ihren Browser, und besuchen Sie die Linuxprinting.org-Druckerlisten-Seite. <http://www.linuxprinting.org/printer_list.cgi>
- Sehen Sie sich die komplette Liste von Druckern in der Datenbank an. <http://www.linuxprinting.org/printer_list.cgi?make=Anyone>.
- Wählen Sie Ihr Modell, und klicken Sie auf den Link.
- Sie landen auf einer Seite, die alle funktionierenden Treiber für dieses Modell auflistet (es gibt für alle Drucker zumindest *einen* empfohlenen Treiber. Probieren Sie den zuerst aus).
- In unserem Fall (HP LaserJet 4 Plus) landen wir beim Standard-Treiber für den HP-LaserJet 4 Plus. <http://www.linuxprinting.org/show_printer.cgi?recnum=HP-LaserJet_4_Plus>
- Der empfohlene Treiber ist ljet4.
- Verschiedene Links werden hier angeboten. Sie sollten sie alle besuchen, falls Sie noch nicht mit der Linuxprinting.org-Datenbank vertraut sind.
- Es gibt einen Link auf die Datanbank-Seite für ljet4. <http://www.linuxprinting.org/show_driver.cgi?driver=ljet4> Auf der Seite des Treibers finden Sie wichtige und detaillierte Informationen, wie Sie den Treiber mit den verschiedenen Spoolern verwenden können.
- Ein weiterer Link führt Sie auf die Homepage des Treibers oder dessen Autors.
- Wichtige Links sind diejenigen, die Ihnen Hinweise und Anleitungen zu CUPS <http://www.linuxprinting.org/cups-doc.html>, PDQ <http://www.linuxprinting.org/pdq-doc.html>, LPD, LPRng und GNUlpr <http://www.linuxprinting.org/lpd-doc.html> geben, genauso wie zu PPR <http://www.linuxprinting.org/ppr-doc.html> oder „*spooler-freiem*“ Drucken. <http://www.linuxprinting.org/direct-doc.html>
- Sie können das PPD in Ihrem Browser mit folgendem Link ansehen: <http://www.linuxprinting.org/ppd-o-matic.cgi?driver=ljet4&printer=HP-LaserJet_4_Plus&show=1>

- Und das Wichtigste ist: Sie können das PPD <`http://www.linuxprinting.org/ppd-o-matic.cgi?driver=ljet4&printer=HP-LaserJet_4_Plus&show=0`> auch generieren und herunterladen.
- Das PPD enthält all die Informationen, um unseren Drucker und den Treiber zu verwenden; sobald es installiert ist, arbeitet es für den Anwender transparent. Sie brauchen später nur noch die Auflösung, das Papierformat usw. aus dem Web-basierenden Menü, dem Druck-GUI-Dialog oder auf der Befehlszeile auswählen.
- Wenn Sie auf der Treiber- Seite <`http://www.linuxprinting.org/show_driver.cgi?driver=ljet4`> angelangt sind, können Sie den „*PPD-O-Matic*“-Online-PPD-Generator verwenden.
- Wählen Sie das genaue Modell aus, wählen Sie **Download** oder **Display PPD file**, und klicken Sie auf **Generate PPD file**.
- Wenn Sie die PPD-Datei aus der Broswer-Ansicht speichern, verwenden Sie bitte nicht Cut and Paste (da dies eventuell die Zeilenenden und Tabulatoren beschädigt, was das PPD eventuell daran hindert, seine Pflicht zu erfüllen), sondern verwenden Sie **Speichern unter...** aus dem Menü Ihres Browsers. (Am besten ist die Verwendung der Option **Download** direkt auf der Webseite).
- Ein weiterer interessanter Teil jeder Treiber-Seite ist der Button **Show execution details**. Wenn Sie Ihr Druckermodell wählen und diesen Button klicken, wird eine komplette Ghostscript-Befehlszeile angezeigt, die alle verfügbaren Optionen für diese Drucker/Treiber-Kombination aufzählt. Dies ist eine gute Möglichkeit, „*Ghostscript durch Anwendung zu erlernen*“. Es ist außerdem ein hervorragender Spickzettel für alle erfahrenen Anwender, die eine gute Befehlszeile für irgendein verdammtes Druck-Skript rekonstruieren müssen, sich aber nicht mehr an die exakte Syntax erinnern.
- Irgendwann während Ihres Besuchs bei Linuxprinting.org speichern Sie Ihre PPD-Datei unter einem passenden Platz auf Ihrer Festplatte, sagen wir `/pfad/zu/ihrer.ppd`. (Wenn Sie es vorziehen, Ihre Drucker unter Verwendung des CUPS-Web-Interface zu installieren, speichern Sie das PPD in `/usr/share/cups/model/` und starten CUPS neu.)
- Dann installieren Sie den Drucker mit einer entsprechenden Befehlszeile, wie dieser:

```
root# lpadmin -p laserjet4plus -v parallel:/dev/lp0 -E \
   -P pfad/zu/mein-drucker.ppd
```

- Für alle neuartigen „*Foomatic-PPDs*“ von Linuxprinting.org brauchen Sie auch den speziellen CUPS-Filter namens foomatic-rip.
- Das foomatic-rip-Perl-Skript selbst gibt ziemlich interessanten Lesestoff <`http://www.linuxprinting.org/foomatic2.9/download.cgi?filename=foomatic-rip&show=1`> ab, da es durch Kamppeters Inline-Kommentare gut dokumentiert ist (sogar Nicht-Perl-Hacker werden einiges über das Drucken lernen, wenn sie es lesen).
- Speichern Sie foomatic-rip entweder direkt in `/usr/lib/cups/filter/foomatic-rip` oder sonstwo in Ihren $PATH (und vergessen Sie nicht, es für alle ausführbar zu

setzen). Verwenden Sie auch hier nicht Cut and Paste, sondern verwenden Sie den entsprechenden Link oder den Menü-Eintrag **Speichern unter ...** Ihres Browsers.

- Wenn Sie foomatic-rip in Ihrem $PATH speichern, legen Sie einen Symlink an:

```
root# cd /usr/lib/cups/filter/ ; ln -s 'which foomatic-rip'
```

CUPS wird diesen neu verfügbaren Filter beim Neustart von cupsd entdecken.

Sobald Sie in eine Queue drucken, die mit dem Foomatic-PPD installiert wurde, fügt CUPS die entsprechenden Befehle und Kommentare in die resultierende PostScript-Datei ein. foomatic-rip kann diese lesen und mit ihnen umgehen, und verwendet einige speziell codierte Foomatic-Kommentare, die in die Auftragsdatei eingebettet sind. Diese werden wiederum dazu verwendet (transparent für Sie, den Anwender), um die komplizierte Ghostscript-Befehlszeile zu konstruieren, die dem Druckertreiber exakt mitteilt, wie die ausgegebenen Rasterdaten auszusehen haben und welche Druckerbefehle in den Datenstrom einzubetten sind. Sie brauchen:

- Eine „*foomatic+irgendwas*“-PPD — aber das ist nicht genug, um mit CUPS zu drucken (es ist nur *eine* wichtige Komponente).
- Das *foomatic-rip*-Filter-Skript (Perl) in `/usr/lib/cups/filters/`.
- Perl, damit foomatic-rip laufen kann.
- Ghostscript (weil es, kontrolliert von der Kombination PPD/foomatic-rip, die Hauptarbeit macht), um die passenden Rasterdaten für Ihr Druckermodell zu produzieren.
- Ghostscript *muss* (abhängig von Ihrem Treiber/Modell) Unterstützung für ein bestimmtes Gerät mitbringen, das den gewählten Treiber für Ihr Modell repräsentiert (wie von **gs -h** gezeigt).
- foomatic-rip braucht eine neue Version PPDs (PPD-Versionen für cupsomatic funktionieren nicht mit foomatic-rip).

18.12 Seitenabrechnung mit CUPS

Es gibt oft Nachfragen bezüglich Druck-Quota, durch die Samba-Benutzer (also Windows-Clients) nicht mehr als eine bestimmte Anzahl von Seiten oder Datenmenge pro Tag, Woche oder Monat drucken dürfen sollen. Dieses Feature hängt vom eingesetzten Drucksystem ab. Sambas Aufgabe ist es, die Druckaufträge von den Clients zu empfangen (gefiltert *oder* ungefiltert) und diese an das Drucksystem weiterzugeben.

Natürlich könnte man sich so etwas mit seinen eigenen Skripten zusammenbauen. Aber es gibt CUPS. CUPS unterstützt Quota, die anhand der Auftragsgröße, der Anzahl der Seiten oder beidem festgelegt werden können und jede zeitliche Periode umspannen können, die Sie festlegen wollen.

18.12.1 Quota einrichten

Dies ist ein Beispiel, wie root ein Druck-Quotum in CUPS einrichten könnte, unter der Annahme, dass es einen Drucker namens „*quotadrucker*“ gibt:

```
root# lpadmin -p quotadrucker -o job-quota-period=604800 \
   -o job-k-limit=1024 -o job-page-limit=100
```

Dies würde jeden einzelnen Benutzer darauf beschränken, 100 Seiten oder 1024 KB (was auch immer zuerst eintrifft) innerhalb der letzten 604800 Sekunden (entspricht einer Woche) zu drucken.

18.12.2 Korrektes und inkorrektes Abrechnen

Damit CUPS richtig zählt, muss die Druckdatei durch den CUPS-pstops-Filter laufen; ansonsten verwendet es einen Ersatzwert von „*eins*“. Manche Druckdateien passieren diesen Filter nicht (z.B. Bilddateien), jedoch sind diese ohnehin meist einseitige Aufträge. Das bedeutet: Aufträge von proprietären Treibern (die auf den Clients laufen), die von CUPS/Samba als „*raw*“ weitergegeben werden (also ohne Filterung), werden auch als einseitige Aufträge gezählt!

Sie müssen PostScript von den Clients senden (d.h., dort einen PostScript-Treiber ausführen), um eine Chance auf korrekte Abrechnung zu bekommen. Wenn der Drucker ein Nicht-PS-Modell ist, müssen Sie CUPS die Wandlung der Auftragsdatei in ein druckfertiges Format für den Zieldrucker durchführen lassen. Dies funktioniert derzeit für ungefähr eintausend verschiedene Druckermodelle. Linuxprinting hat eine Treiber- Liste. <`http://www.linuxprinting.org/printer_list.cgi`>

18.12.3 Adobe- und CUPS-PostScript-Treiber für Windows-Clients

Vor CUPS 1.1.16 hatten Sie nur diee Option, den Adobe-PostScript-Treiber auf den Windows-Clients zu verwenden. Die Ausgabe dieses Treibers wurde auf der Seite von CUPS/Samba nicht immer durch den **pstops**-Filter geschleust und daher auch nicht korrekt gezählt. (Das lag daran, dass oft, abhängig vom verwendeten PPD, ein PJL-Header vor das tatsächliche PostScript gesetzt wurde, was CUPS zum Überspringen von **pstops** veranlasste und es direkt zum **pstoraster**-Schritt brachte).

Seit CUPS 1.1.16 können Sie den CUPS-PostScript-Treiber für Windows NT/200x/XP-Clients verwenden (der im Download-Bereich von `http://www.cups.org/` als `cups-samba-1.1.16.tar.gz` zu finden ist). Er funktioniert *nicht* für Windows 9x/ME-Clients, garantiert jedoch:

- keinen PJL-Header zu schreiben,
- nach wie vor alle PJL-Optionen zu lesen und zu unterstützen, die im Treiber-PPD benannt sind,
- dass die Datei durch den **pstops**-Filter auf dem CUPS/Samba-Server gefiltert wird und

- die korrekte Seitenzählung der Druckdatei.

Sie können mehr über das Setup dieser Kombination in der Manpage für **cupsaddsmb** lesen (die nur vorhanden ist, wenn CUPS installiert ist, und nur aktuell seit CUPS 1.1.16 ist).

18.12.4 Die Syntax der Datei page_log

CUPS protokolliert in `page_log` für jede Seite eines Auftrags folgende Punkte:

- Druckername
- Benutzername
- Auftrags-ID
- Die Zeit des Drucks
- Die Seitenzahl
- Die Anzahl der Kopien
- Einen Informations-String für die Verrechnung (optional)
- Den Host, der den Auftrag gesendet hat (seit Version 1.1.19)

Hier sehen Sie einen Auszug aus der Datei `page_log` meines CUPS-Servers, um das Format und die enthaltenen Begriffe zu illustrieren:

```
tec_IS2027 kurt 401 [22/Apr/2003:10:28:43 +0100] 1 3 #marketing 10.160.50.13
tec_IS2027 kurt 401 [22/Apr/2003:10:28:43 +0100] 2 3 #marketing 10.160.50.13
tec_IS2027 kurt 401 [22/Apr/2003:10:28:43 +0100] 3 3 #marketing 10.160.50.13
tec_IS2027 kurt 401 [22/Apr/2003:10:28:43 +0100] 4 3 #marketing 10.160.50.13
Dig9110 boss 402 [22/Apr/2003:10:33:22 +0100] 1 440 finance-dep 10.160.51.33
```

Dies war die Auftrags-ID *401*, die auf *tec_IS2027* vom Benutzer *kurt* gedruckt wurde: ein 64-Seiten-Auftrag, der in 3 Kopien gedruckt, *#marketing* in rechnung gestellt und von der IP-Adresse `10.160.50.13.` gesendet wurde. Der nächste Auftrag hatte die ID *402*, wurde vom Benutzer *boss* von der IP-Adresse `10.160.51.33` gesendet, druckte von einer Seite 440 Kopien und soll *finance-dep* in Rechnung gestellt werden.

18.12.5 Mögliche Mängel

Welche Mängel gibt es bei diesem Quota-System?

- Die oben genannten (falsch protokollierter Auftrag im Fall von Drucker-Hardware-Ausfall usw.).
- In Wirklichkeit zählt CUPS die Auftragsseiten, die in der *Software* verarbeitet werden (also durch den RIP gehen), und nicht die physischen Seiten, die den Drucker verlassen. Daher wird der Seitenzähler, wenn es bei der ersten von tausend Seiten einen Papierstau gibt, der den Drucker zum Abbruch des Auftrags zwingt, nach wie vor auf 1000 Seiten für diesen Auftrag stehen.

- Alle Quota sind dieselben für alle Benutzer (es ist keine Flexibilität vorhanden, um dem Boss ein höheres Quotum als dem Angestellten zu geben), und es gibt keine Unterstützung für Gruppen.
- Keine Möglichkeit, um die momentane Balance oder den „*verbrauchten*“ Anteil des aktuellen Quotums auszulesen.
- Ein Benutzer, der 99 Seiten eines 100-Seiten-Quotums verbraucht hat, ist nach wie vor imstande, einen 1000-Seiten-Auftrag zu senden und zu drucken.
- Ein Benutzer, dem ein Auftrag abgelehnt wird, da er sein Quotum erreicht hat, bekommt keine verständliche Fehlermeldung von CUPS außer „*client-error-not-possible*“.

18.12.6 Zukünftige Entwicklungen

Dies ist das beste derzeit verfügbare System, und es gibt bedeutende Verbesserungen, die in Entwicklung für CUPS 1.2 sind:

- Die Seitenzählung wird in die Backends verlagert (diese reden direkt mit dem Drucker und erhöhen den Zähler synchron mit dem tatsächlichen Druckvorgang; daher wird ein Papierstau bei der fünften Seite auch den Zähler bei fünf stoppen).
- Quota werden flexibler behandelt werden.
- Möglicherweise wird es Unterstützung dafür geben, dass sich Benutzer schon vorab über ihre Konten informieren können.
- Vielleicht gibt es dann auch eine Unterstützung für andere Werkzeuge zu diesem Thema.

18.13 Zusätzliches Material

Eine Druckerqueue mit *keinem* assoziierten PPD ist ein „*raw*“-Drucker, und alle Dateien gehen direkt an den Drucker, sobald sie vom Spooler empfangen werden. Die Ausnahme sind die Dateien vom Typ *application/octet-stream*, die das Feature pass-through aktiviert haben müssen. „*Raw*“-Queues führen überhaupt keine Filterung durch, sie geben die Datei direkt an das CUPS-Backend weiter. Dieses Backend ist dafür verantwortlich, die Daten an das Gerät zu senden (wie in der „*device URI*“-Notation: `lpd://`, `socket://`, `smb://`, `ipp://`, `http://`, `parallel:/`, `serial:/`, `usb:/` und so weiter).

cupsomatic/Foomatic sind *keine* nativen CUPS-Treiber, und sie werden nicht mit CUPS geliefert. Sie sind ein Dritthersteller-Zusatz, der auf Linuxprinting.org entwickelt wird. Als solches sind sie ein brillanter Hack, um alle Modelle (angetrieben von Ghostscript-Treibern/Filtern in traditionellen Spoolern) auch via CUPS zu betreiben, und zwar mit derselben Qualität (gut oder schlecht!) wie in diesen anderen Spoolern. *cupsomatic* ist nur ein Hilfsmittel, um an dieser Stelle in der CUPS-Filterkette eine Ghostscript-Befehlszeile auszuführen, wo normalerweise der native CUPS-Filter *pstoraster* „*anspringen*“ würde. cupsomatic übergeht pstoraster, nimmt die Druckdatei von CUPS in Beschlag und leitet sie durch Ghostscript um. CUPS akzeptiert das, weil die zugeordnete cupsomatic/foomatic-PPD Folgendes angibt:

```
*cupsFilter:  "application/vnd.cups-postscript 0 cupsomatic"
```

Diese Zeile bewegt CUPS dazu, die Datei an cupsomatic zu übergeben, sobald es sie erfolgreich in den MIME-Typ *application/vnd.cups-postscript* umgewandelt hat. Diese Umwandlung erfolgt nicht für Aufträge von Windows, die automatisch als *application/octet-stream* typisiert werden, (((mit den begleitenden Änderungen in `/etc/cups/mime.types` – Bezug?))).

CUPS ist weitgehend konfigurierbar und flexibel, sogar was seinen Filtermechanismus betrifft. Ein weiterer „*Workaround*“ in manchen Situationen wäre es, Einträge in `/etc/cups/mime.types` zu haben, wie folgt:

```
application/postscript           application/vnd.cups-raw  0  -
application/vnd.cups-postscript  application/vnd.cups-raw  0  -
```

Dies würde verhindern, dass jegliche PostScript-Dateien gefiltert werden (sie werden dann eigentlich durch den virtuellen Filter *nullfilter* gefiltert, bezeichnet mit „-“). Das könnte nur für PS-Drucker hilfreich sein. Wenn Sie PS-Code auf Nicht-PS-Druckern drucken wollen (sofern diese ASCII-Textdruck beherrschen), könnte ein Eintrag wie dieser helfen:

```
*/*           application/vnd.cups-raw  0  -
```

Er schickt *alle* Dateien ohne weitere Bearbeitung an das Backend weiter.

Sie könnten den folgenden Eintrag haben:

```
application/vnd.cups-postscript application/vnd.cups-raw 0 \
   my_PJL_stripping_filter
```

Sie werden einen *mein_PJL_entfernungs_filter* schreiben müssen (dies könnte ein Shell-Skript sein), der die PS-Daten analysiert und das unerwünschte PJL entfernt. Dies muss konform zum CUPS-Filter-Design passieren (vor allem muss es die Parameter Druckername, Job-ID, Benutzername, Jobtitle, Kopien, Druckoptionen und eventuell den Dateinamen empfangen und weitergeben). Der Filter wird als für alle ausführbar in `/usr/lib/cups/filters/` installiert und wird von CUPS aufgerufen, wenn es einen MIME-Typen *application/vnd.cups-postscript* erkennt.

CUPS kann mit *-o job-hold-until=indefinite* umgehen. Das hält den Auftrag in der Queue auf Stillstand. Er wird nur auf manuelle Veranlassung des Druck-Operators gedruckt. Dies ist eine Anforderung in vielen Reproduktionsabteilungen, wo ein paar wenige Operatoren die Aufträge von vielen hundert Benutzern auf irgendeiner großen Maschine verwalten, wo keinem Benutzer direkter Zugriff gestattet ist (wo z.B. die Operatoren das richtige Papier laden müssen, bevor sie den 10.000-Seiten-Auftrag starten, der vom Marketing für das Mailing eingetroffen ist, usw.).

18.14 Auto-Löschen oder Erhaltung der CUPS-Spool-Dateien

Samba-Druckdateien durchlaufen zwei Spool-Verzeichnisse. Eines ist das Eingangsverzeichnis, das von Samba verwaltet wird. (Es ist im Parameter path = /var/spool/samba im Abschnitt *[printers]* von `smb.conf` festgelegt). Das andere ist das Spool-Verzeichnis Ihres UNIX-Drucksystems. Für CUPS ist das normalerweise `/var/spool/cups/`, das in der Anweisung `RequestRoot /var/spool/cups` in der Datei `cupsd.conf` gesetzt ist.

18.14.1 Erklärung von CUPS-Konfigurationseinstellungen

Einige wichtige Parameter in der CUPS-Konfigurationsdatei `cupsd.conf` sind:

PreserveJobHistory Yes Dies belässt einige Details von Aufträgen im „*Gedächtnis*“ von cupsd (es hält die Dateien c12345, c12346 usw. im CUPS-Spool-Verzeichnis, die einen ähnlichen Job machen wie die altmodischen BSD-LPD-Kontrolldateien). Der voreingestellte Wert dieses Parameters ist „*Yes*“.

PreserveJobFiles Yes Das belässt die Auftragsdateien selbst im „*Gedächtnis*“ von cupsd (es hält die Dateien d12345, d12346 etc. im CUPS-Spool-Verzeichnis). Der voreingestellte Wert dieses Parameters ist „*No*“.

„MaxJobs 500“ Diese Anweisung kontrolliert die maximale Anzahl von Aufträgen, die im Speicher gehalten werden. Sobald die Anzahl der Aufträge das Limit erreicht, wird der älteste abgeschlossene Auftrag automatisch aus dem System entfernt, um Platz für den neuen zu machen. Wenn alle Aufträge nach wie vor in Schwebe oder aktiv sind, wird der neue Auftrag abgelehnt. Setzt man dieses Maximum auf 0, wird diese Funktionalität deaktiviert. Der voreingestellte Wert dieses Parameters ist 0.

(Es gibt auch noch zusätzliche Einstellungen für *MaxJobsPerUser* und *MaxJobsPerPrinter*...)

18.14.2 Vorbedingungen

Damit alles so funktioniert wie besprochen, brauchen Sie drei Dinge:

- Einen Samba-smbd, der mit `libcups` kompiliert wurde (Sie können das unter Linux mit `ldd 'which smbd'` prüfen.)
- Die Einstellung printing = cups in der Samba-`smb.conf`
- Die Einstellung printcap = cups in der Samba-`smb.conf`

ANMERKUNG

In diesem Fall werden alle anderen manuell gesetzten druckbezogenen Befehle (wie print command, lpq command, lprm command, lppause command oder lpresume command) ignoriert und sollten normalerweise keinerlei Einfluss mehr auf Ihren Druck haben.

18.14.3 Manuelle Konfiguration

Wenn Sie Dinge manuell tun wollen, ersetzen Sie printing = cups durch printing = bsd. Dann kann Ihr manuell gesetzter Befehlssatz funktionieren (ich habe das *nicht* getestet), und print command = lp -d %P %s; rm %s"könnte das tun, was Sie brauchen.

18.15 Aus CUPS auf Windows-Drucker drucken

Von Zeit zu Zeit taucht die Frage auf, wie man *von* Samba *auf* einen Windows-Drucker druckt. Normalerweise erfolgt die lokale Verbindung vom Windows-Rechner zum Drucker via USB- oder Parallel-Kabel, aber das macht Samba nichts aus. Hier muss nur eine SMB-Verbindung zum Windows-Rechner geöffnet werden. Natürlich muss der Drucker zuvor freigegeben werden. Wie Sie bereits gelernt haben, verwendet CUPS *Backends*, um mit den Druckern und anderen Servern zu kommunizieren. Um mit unter Windows freigegebenen Druckern zu kommunizieren, müssen Sie das Backend `smb` (was für eine Überraschung!) verwenden. Prüfen Sie, ob es dieses im CUPS-Backend-Verzeichnis gibt. Dieses liegt üblicherweise in `/usr/lib/cups/backend/`. Sie sollten dort eine Datei namens `smb` vorfinden. Diese sollte ein Symlink auf `smbspool` sein, und diese Datei muss existieren und ausführbar sein:

```
root# ls -l /usr/lib/cups/backend/
total 253
drwxr-xr-x    3 root   root     720 Apr 30 19:04 .
drwxr-xr-x    6 root   root     125 Dec 19 17:13 ..
-rwxr-xr-x    1 root   root   10692 Feb 16 21:29 canon
-rwxr-xr-x    1 root   root   10692 Feb 16 21:29 epson
lrwxrwxrwx    1 root   root       3 Apr 17 22:50 http -> ipp
-rwxr-xr-x    1 root   root   17316 Apr 17 22:50 ipp
-rwxr-xr-x    1 root   root   15420 Apr 20 17:01 lpd
-rwxr-xr-x    1 root   root    8656 Apr 20 17:01 parallel
-rwxr-xr-x    1 root   root    2162 Mar 31 23:15 pdfdistiller
lrwxrwxrwx    1 root   root      25 Apr 30 19:04 ptal -> /usr/sbin/ptal-cups
-rwxr-xr-x    1 root   root    6284 Apr 20 17:01 scsi
lrwxrwxrwx    1 root   root      17 Apr  2 03:11 smb -> /usr/bin/smbspool
-rwxr-xr-x    1 root   root    7912 Apr 20 17:01 socket
-rwxr-xr-x    1 root   root    9012 Apr 20 17:01 usb
```

```
root# ls -l `which smbspool`
-rwxr-xr-x    1 root   root  563245 Dec 28 14:49 /usr/bin/smbspool
```

Wenn der Symlink nicht existiert, legen Sie ihn an:

```
root# ln -s `which smbspool` /usr/lib/cups/backend/smb
```

smbspool wurde von Mike Sweet (von den CUPS-Leuten) geschrieben. Es ist in Samba enthalten. Es kann auch zum Drucken auf andere Subsysteme als CUPS verwendet werden, um Aufträge an Windows-Druckfreigaben zu spoolen. Um den Drucker *winprinter* unter CUPS einzurichten, müssen Sie einen Treiber dafür haben. Prinzipiell bedeutet das, dass die Druckdaten auf dem CUPS/Samba-Rechner in ein für den Drucker verdaubares Format gewandelt werden müssen (der Windows-Rechner ist unfähig, irgendwelche von Ihnen gesendete Daten zu konvertieren). Das bedeutet auch, dass Sie imstande sein sollten, auf den Drucker zu drucken, wenn er direkt an den CUPS/Samba-Rechner angeschlossen wäre. Das ist es auch, was Sie zur Fehlersuche tun sollten, um zu prüfen, ob dieses Glied der Verarbeitungskette intakt ist. Dann fahren Sie damit fort, die Netzwerk-Verbindung/Authentifikation zum/am Windows-Rechner zu prüfen, usw.

Um einen Drucker mit dem Backend *smb* unter CUPS zu installieren, verwenden Sie diesen Befehl:

```
root# lpadmin -p winprinter -v smb://WINDOWSNETBIOSNAME/printersharename \
  -P /path/to/PPD
```

Das PPD muss imstande sein, CUPS anzuweisen, die Druckdaten für das Zielgerät zu generieren. Für PS-Drucker verwenden Sie einfach das PPD, das mit dem Windows NT-PostScript-Treiber verwendet würde. Aber was machen Sie, wenn der Drucker nur mit einem Passwort zugänglich ist? Oder wenn der Drucker-Server Mitglied einer anderen Arbeitsgruppe ist? Dafür wurde vorgesorgt: Sie können die erforderlichen Parameter als Teil der `smb://` Geräte-URI angeben:

- `smb://ARBEITSGRUPPE/WINDOWSNETBIOSNAME/druckerfreigabenname`
- `smb://benutzername:passwort@ARBEITSGRUPPE/WINDOWSNETBIOSNAME/druckerfreigabenname`
- `smb://benutzername:passwort@WINDOWSNETBIOSNAME/druckerfreigabenname`

Beachten Sie, dass die Geräte-URI in der Prozessliste des Samba-Servers sichtbar ist (d.h., wenn jemand den Befehl **ps -aux** unter Linux verwendet), sogar wenn der Benutzername und die Passwörter bereinigt werden, bevor sie in die Logfiles geschrieben werden. Also ist dies eine inhärent unsichere Option, jedoch ist es die einzige. Verwenden Sie dies nicht, wenn Sie Ihre Passwörter schützen wollen. Geben Sie besser den Drucker so frei, dass man kein Passwort benötigt! Das Drucken wird nur funktionieren, wenn Sie eine funktionierende Netbios-Namensauflösung haben. Beachten Sie, dass dies eine Eigenschaft von CUPS ist und Sie nicht notwendigerweise smbd laufen lassen müssen.

18.16 Mehr CUPS-Filterketten

Die folgenden Diagramme „*enthüllen*“, wie CUPS mit Druckaufträgen umgeht.

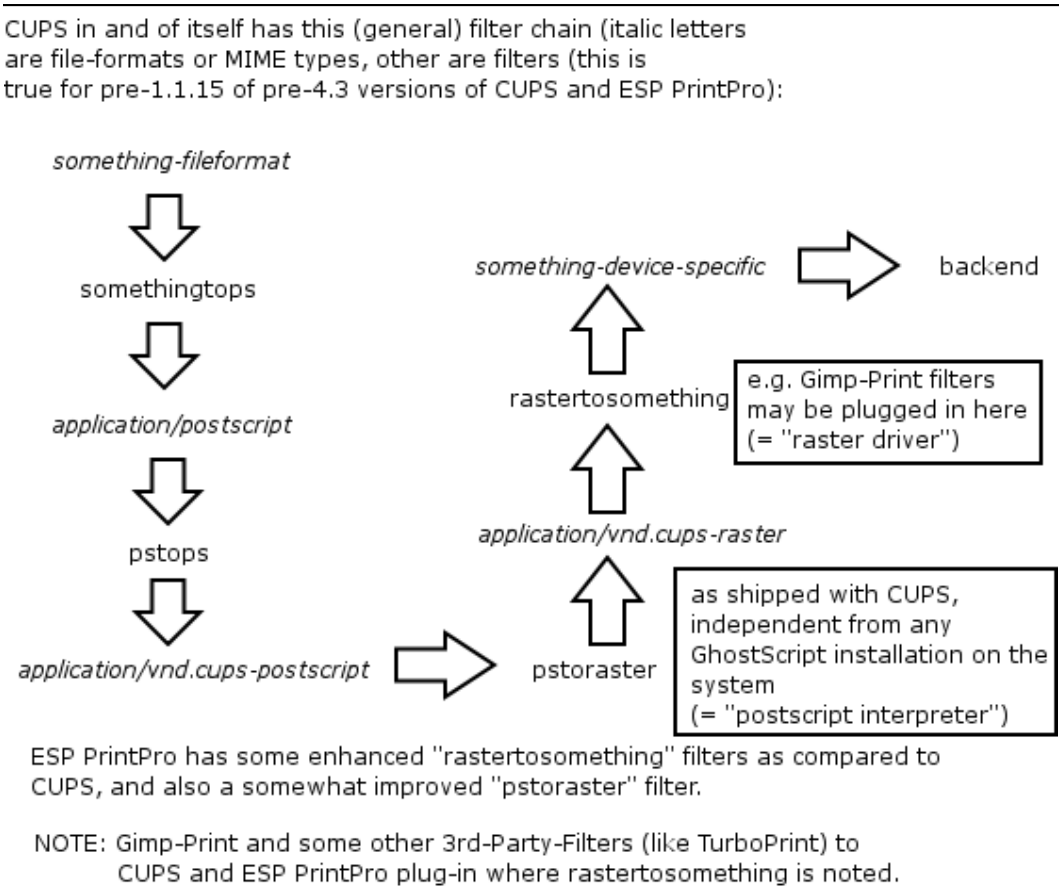

CUPS in and of itself has this (general) filter chain (italic letters
are file-formats or MIME types, other are filters (this is
true for pre-1.1.15 of pre-4.3 versions of CUPS and ESP PrintPro):
something-fileformat
somethingtops
application/postscript
pstops
application/vnd.cups-postscript
pstoraster
application/vnd.cups-raster
rastertosomething
something-device-specific
backend
e.g. Gimp-Print filters
may be plugged in here
(= "raster driver")
as shipped with CUPS,
independent from any
GhostScript installation on the
system
(= "postscript interpreter")
ESP PrintPro has some enhanced "rastertosomething" filters as compared to
CUPS, and also a somewhat improved "pstoraster" filter.
NOTE: Gimp-Print and some other 3rd-Party-Filters (like TurboPrint) to
CUPS and ESP PrintPro plug-in where rastertosomething is noted.

Figure 18.16. Filterkette 1

18.17 Gängige Fehler

18.17.1 Ein Windows 9x/ME-Client kann keinen Treiber installieren

Für Windows 9x/ME benötigen die Clients Druckernamen, die maximal acht Zeichen lang sind (oder „*8 plus 3 Zeichen Suffix*“); andernfalls werden die Treiberdateien nicht übertragen, wenn Sie sie von Samba herunterladen wollen.

18.17.2 „*cupsaddsmb*“ fragt immer wieder nach dem root-Passwort

Verwenden Sie security = user? Haben Sie **smbpasswd** verwendet, um root ein Samba-Konto zu geben? Sie können zwei Dinge tun: ein anderes Terminal öffnen und **smbpasswd -a root** ausführen, um das Konto anzulegen und im ersten Terminal damit fortfahren, das neue Passwort dort einzugeben. Oder Sie brechen die Schleife ab, indem Sie zweimal ENTER drücken (ohne zu versuchen, ein Passwort einzugeben).

Wenn der Fehler „*tree connect failed: NT_STATUS_BAD_NETWORK_NAME*“ lautet, haben Sie vielleicht vergessen, das Verzeichnis `/etc/samba/drivers` anzulegen.

18.17.3 „*cupsaddsmb*“-Fehler

Die Verwendung von „*cupsaddsmb*“ führt zur Meldung „*No PPD file for printer...*“, obwohl die Datei vorhanden ist. Was kann das Problem sein?

Haben Sie die Drucker-Freigabe in CUPS aktiviert? Das heißt, haben Sie einen Abschnitt *<Location /printers>....</Location>* in der Datei `cupsd.conf` Ihres CUPS-Servers, die dem Host, von dem aus Sie „*cupsaddsmb*“ auszuführen versuchen, den Zugriff erlaubt? Es *könnte* ein Problem sein, wenn Sie cupsaddsmb übers Netz oder mit dem Parameter `-h` verwenden: `cupsaddsmb -H sambaserver -h cupsserver -v printername`.

Ist die Anweisung *TempDir* in `cupsd.conf` auf einen gültigen Wert gesetzt und schreibbar?

18.17.4 Der Client kann sich nicht mit dem Samba-Drucker verbinden

Verwenden Sie **smbstatus**, um zu prüfen, welcher Benutzer Sie aus der Sicht von Samba sind. Haben Sie die Rechte, um in die Freigabe *[print$]* zu schreiben?

18.17.5 Neue Probleme: Wiederverbindung mit anderem Konto unter Windows 200x/XP

Sobald Sie als falscher Benutzer verbunden sind (z.B. als `nobody`, was oft geschieht, wenn Sie map to guest = bad user gesetzt haben), wird der Windows Explorer es nicht akzeptieren, wenn Sie sich als ein anderer Benutzer anzumelden versuchen. Nicht ein Byte wird zu Samba übertragen werden, aber Sie werden immer noch eine dumme Fehlermeldung sehen, die Sie glauben lässt, dass Samba den Zugriff verweigert hat. Verwenden Sie **smbstatus**, um nach aktiven Verbindungen zu sehen. Killen Sie die PIDs. Sie können sich noch immer nicht neu verbinden und bekommen die gefürchtete Meldung `You can't connect with a second account from the same machine`, sobald Sie es versuchen. Und Sie sehen kein einziges Byte bei Samba ankommen (sehen Sie sich die Logs an; verwenden Sie „*ethereal*“), das einen neuerlichen Verbindungsversuch anzeigt. Schließen Sie alle Explorer-Fenster. Das lässt Windows vergessen, was es in seinem Speicher als aufgebaute Verbindungen gepuffert hat. Dann verbinden Sie sich neu als der „*richtige*“ Benutzer. Die beste Methode ist es, ein DOS-Terminal-Fenster zu verwenden und *zuerst* `net use z: \\GANDALF\print$ /user:root` auszuführen. Überprüfen Sie mit **smbstatus**, dass Sie mit einem anderen Konto angemeldet sind. Jetzt öffnen Sie den Folder **Drucker und Faxgeräte** (auf dem Samba-Server in der

Windows XP behandelt SMB-Drucker auf einer #Gtextglqq¿per-user#Gtextgrqq¿-Basis. Das bedeutet, dass jeder Benutzer den Drucker selbst installieren muss. Um einen Drucker zu haben, der für jeden verfügbar ist, möchten Sie vielleicht die integrierten IPP-Client-Fähigkeiten von Windows XP nutzen. Fügen Sie einen Drucker mit dem Druck-Pfad http://cupsserver:631/printers/druckername hinzu. Wir suchen nach wie vor nach einer Lösung dieses Problems. Vielleicht könnte ein Anmelde-Skript automatisch Drucker für alle Benutzer installieren.

(((Print Change Notify Functions on NT-clients)))
For print change, notify functions on NT++ clients.(((übersetzen))) Diese müssen zuerst den Server-Dienst ausführen. (In XP wurde er in Datei- #Gtextampersand¿ und Druckerfreigabe für Microsoft-Netzwerke umbenannt).

Win XP-SP1
Win XP-SP1 führte eine Point-and-Print-Beschränkungsrichtlinie ein (diese Beschränkung gilt nicht für die Benutzergruppen #Gtextglqq¿Administrator#Gtextgrqq¿ oder #Gtextglqq¿Power User#Gtextgrqq¿). Im Gruppenrichtlinien-Editor gehen Sie auf Benutzerkonfiguration -> Administrative Vorlagen -> Systemsteuerung -> Drucker. Diese Richtlinie ist automatisch aktiviert und auf Benutzer können Point and Print nur für Computer in der eigenen Gesamtstruktur verwenden gesetzt. Sie müssen dies eventuell auf Deaktiviert oder Point and Print nur mit folgenden Servern setzen, um Treiber-Downloads von Samba zu ermöglichen.

Drucker-Optionen für alle Benutzer können nicht unter Windows 200x/XP gesetzt werden
Wie machen Sie das? Ich wette, auf die falsche Art (es ist auch nicht einfach herauszufinden). Es gibt drei verschiedene Arten, Sie zu einem Dialog zu bringen, der scheinbar all diese Dinge setzen kann. Alle drei Dialoge sehen gleich aus, jedoch tut nur einer das, was Sie beabsichtigen. Sie müssen Administrator oder Druck-Administrator sein, um dies für alle Benutzer tun zu können. Hier sehen Sie, wie ich das in XP mache:
[A] Die erste falsche Art: Öffnen von Drucker und Faxgeräte.
Rechtsklick auf den Drucker (netzwerkdrucker auf cupshost) und Auswahl von Druckeinstellungen im Kontextmenü.
Sehen Sie sich diesen Dialog genau an, und versuchen Sie, sich genau zu merken, wie er aussieht.
Die zweite falsche Art: Öffnen von Drucker und Faxgeräte.
Rechtsklick auf den Drucker (netzwerkdrucker auf cupshost) und Auswahl von Eigenschaften im Kontextmenü.
Klick auf Allgemein.
Klick auf Druckeinstellungen...
Ein neuer Dialog öffnet sich. Halten Sie diesen Dialog geöffnet, und gehen Sie zurück zum ersten Dialog.
Die dritte und richtige Art: Öffnen von Drucker und Faxgeräte.
Klick auf Erweitert. (Wenn alles #Gtextglqq¿grau ist#Gtextgrqq¿, dann sind Sie nicht als Benutzer mit ausreichenden Rechten angemeldet).
Klicken Sie auf den Button Druckeinstellungen.
Auf irgendeiner der beiden erscheinenden #Gtextglqq¿Karteikarten#Gtextgrqq¿ klicken Sie auf den Button Erweitert....
Ein neuer Dialog öffnet sich. Vergleichen Sie ihn mit dem anderen, identisch aussehenden aus Variante #Gtextglqq¿A#Gtextgrqq¿ oder #Gtextglqq¿B#Gtextgrqq¿.
Sehen Sie irgendeinen Unterschied? Ich auch nicht. Wie auch immer: Nur der letzte Dialog, zu dem Sie nach Befolgung von Variante #Gtextglqq¿C#Gtextgrqq¿ gelangt sind, wird all die Einstellungen dauerhaft speichern und zu Voreinstellungen für neue Benutzer machen. Wenn Sie wollen, dass alle Clients dieselben Voreinstellungen erhalten, müssen Sie diese Schritte als Administrator (printer admin in smb.conf) durchführen, bevor ein Client den Treiber herunterlädt (die Clients können später ihre per-user-Standards setzen, indem sie die obigen Prozeduren A oder B befolgen).

Die gängigsten Schnitzer in den Treiber-Einstellungen auf Windows-Clients
Verwenden Sie nicht Optimize for Speed, sondern verwenden Sie stattdessen Optimize for Portability (Adobe-PS-Treiber). Verwenden Sie nicht Page Independence: No, sondern verwenden Sie immer Page Independence: Yes (Microsoft PS-Treiber und CUPS-PS-Treiber für Windows NT/200x/XP). Wenn es irgendwelche Probleme mit Schriften gibt, verwenden Sie Download as Softfont into printer (Adobe-PS-Treiber). Wählen Sie für TrueType Download Options Outline. Verwenden Sie PostScript Level 2, wenn Sie Probleme mit einem Nicht-PS-Drucker haben und Sie die Wahl haben.

cupsaddsmb funktioniert nicht mit einem neu installierten Drucker
Symptom: Der letzte Befehl von cupsaddsmb schließt nicht erfolgreich ab. Wenn cmd = setdriver printername printername NT_STATUS_UNSUCCESSFUL zurückgibt, dann wurde der Drucker eventuell noch nicht erfolgreich von Samba erkannt. Erscheint er in

Der Administrator kann keine Drucker f“374r alle lokalen Benutzer installieren

Aktualisierung

Seit Erst-Ver“366ffentlichung dieses Buches in Englisch haben die Samba-Versionen 3.0.1 bis 3.0.7 wichtige Aktualisierungen und “304nderungen erfahren. Die Entwickler beseitigten verschiedene Fehler und schlossen Sicherheitsl“374cken. Viele Modifikationen betrafen auch die Druckfunktionen. Hier eine kurze “334bersicht:

> ['rpcclient adddriver'] akzeptiert jetzt die Angabe der Treiber-Version. Dies erm“366glicht die kontrollierte Installation von 'Kernel Mode'- und 'User Mode'-Druckertreibern. (“304nderung seit 3.0.1) Beispiel: []

root rpcclient localhost -N -U'root-c 'adddriver "Windows NT x86" “357nfotec$_2$105 : $cupsdrv5.dll : infotec_2105.ppd : cupsui5.dll : cups5.hlp : NULL : RAW : NULL"2^{\#}I\prime\#I$

['printing = ...'] ist jetzt nicht mehr 'globaler', sondern 'service level'-Parameter. Dies erlaubt mehr Flexibilit“344t und eine bequemere Verwirklichung eigener Druckbefehle ('print command' in smb.conf), unterschiedlich pro Druckerwarteschlange. (“304nderung seit 3.0.3)

Beispiel: []

printing = sysvprinting = sysv

erlaubt die Angabe von Druckoptionen wie z.B '-o raw' ohne in die Konfiguration des CUPS-Servers eingreifen zu müssen. (neuer Parameter seit 3.0.3)

Beispiel:

```
cups options = 'raw,media=a4,job-sheets=secret,secret'cups options = 'raw,media=a4,jo
```

legt das Zeitintervall in Sekunden fest, in dem Samba die 'printcap' nach neu hinzugekommenen (oder gelöschten) Druckerwarteschlangen untersucht. (neuer Parameter seit 3.0.6)

Beispiel:

```
printcap cache time = 60printcap cache time = 60
```

ermöglicht die Zuordnung eines anderen Namens zu einer Druckerwarteschlange. Dieser Name wird den Windows-Clients gezeigt (Unix-Benutzer sehen den ursprünglichen Namen). (neuer Parameter seit 3.0.6)

Beispiel:

```
root# rpcclient localhost -N   \
```

```
-U'root%secret' \
-c 'setprintername cups_printer "Drucker für Gruppe Marketing"'
```

erlaubt die Verwendung eines von 'localhost' unterschiedlichen CUPS-Servers. Unterschiedliche virtuelle smbd-Prozesse können sogar unterschiedliche cups server verwenden. (neuer Parameter seit 3.0.6) Beispiele:

```
cups server = 10.160.61.60cups server = 10.160.61.60
cups server = cups2.domain.comcups server = cups2.domain.com
```

ist ein neues Migrationstool seit 3.0.3 zum zeitsparenden Klonen und Transfer von Windows-Druckertreibern von einem (Windows- oder Samba-)Printserver zu einem anderen. (neu enthalten seit 3.0.3)

nähere Erläuterungen siehe unten.

18.17.11 'rpcclient adddriver'

Dieses Kommando versuchte in den Versionen vor Samba-3.0.1 automatisch zu erkennen, welchen Druckertreiber-Typ es installieren sollte: Version '2' oder Version '3'. Seit 3.0.1 können Sie die Version explizit angeben.

Windows NT kennt nur die sogenannten 'Version 2'-Treiber. Diese laufen im Kernel-Modus und installieren sich in das Unterverzeichnis '2' der [print]-Freigabe. 'Version 2'-Drucertreiber können wegen ihrer Ausführung im Kernelmodus das komplette Windows-System mit in den Abgrund ziehen, wenn sie abstürzen. Besonders berüchtigt sind hier manche Billigdrucker-Treiber. Hingegen sind dies Adobe- wie auch die Microsoft-PostScript-Treiber der 'Version 2' gut getestet. Sie machen bekanntermassen keinerlei Schwierigkeiten, obwohls sie (auch unter 2K/XP) im Kernelmodus laufen.

Mit Windows 2000 führte Microsoft die 'Version 3'-Treiber ein. Diese laufen im 'Userspace-Modus'. Ein Treiberproblem bringt deshalb nicht mehr den kompletten Rechner zum Absturz. (Windows 2000 und XP können allerdings die älteren 'Version 2'-Treiber in einem 'Kompatibiltätsmodus' ausführen. Dies ist allerdings nur bedenkenlos für die Adobe- oder Microsoft-PS-Treiber zu empfehlen. Falls Sie die Wahl haben, wählen Sie immer die 'Version 3'-Treiber. Diese laufen allerdings nicht auf Windows NT Workstations. Ein Samba-Printserver, der NT-Clients zu bedienen hat, muss die 'Version 2'-Treiber vorrätig halten, damit sie per 'Point'n'Print' installierbar sind.

Der 'rpcclient adddriver' Befehl hat eine leicht geänderte Syntax. Als letzten Parameter übergeben Sie ihm jetzt die Treiber-Version. '3' für Win2000/XP, '2' für WinNT und '0' für Win95/98/ME.

WICHTIG

Gehen Sie bei der Verwendung des 'rpcclient adddriver' sorgfältig vor. Falls Sie die falsche Versionsnummer ('2' oder '3') angeben, ist der Treiber nicht installierbar. Im besten Falle erhalten Sie sofort eine Fehlermeldung. Im weniger günstigen Fall ernten Ihre Anwender die Meldung (((?))) und können den Treiber nicht per 'Point'n'Print' installieren. Und im schlimmsten Fall installiert sich der Treiber zwar auf die Clients, funktioniert jedoch nicht oder bringt diese zum Absturz.

18.17.12 'printing = ...'

CUPS verschafft Ihnen einige Annehmlichkeiten, die andere Drucksysteme nicht bieten können. Innerhalb von Samba erspart es Ihnen sogar die Angabe eines 'print command = ...'-Eintrags in der `smb.conf`. Denn CUPS macht das automatisch richtig...

Mit 'printing = cups' legen Sie in pre-3.0.3-Versionen global fest, dass Ihr Samba-Server CUPS verwenden soll. Dieses gilt dann für alle Drucker und Druckerwarteschlangen.

Da viele Administratoren jedoch gerne einige 'Spezialdrucker' verwenden wollen, die einen eigenen Druckbefehl erfordern, war diese Einschränkung zu unflexibel. Insbesondere die vielen im Umlauf befindlichen 'Virtuellen PDF-Drucker', die mit Hilfe von Ghostscript ihren Windows-Clients PDF-Dateien erzeugen und diese dem Anwender ins eigene Verzeichnis wieder ablegen, waren dadurch nicht ohne 'Klimmzüge' mit CUPS zu verwenden.

Seit 3.0.3 können Sie jeder Druckerwarteschlange ihre eigene Einstellung zuordnen. Denn 'printing = ...' ist jetzt ein sogenannter 'service level'-Paramter, und kein 'globaler' mehr.

Sie können aber nach wie vor 'printing = cups' in die [global]-Sektion der `smb.conf` schreiben. (Sie dürfen alle 'service level' Paramter in den Rang eines globalen befördern – Sie dürfen nur nicht globale Parameter in den service leveln ((()))? verwenden). Ein 'printing = cups' Eintrag in der [global]-Sektion gilt automatisch für alle Drucker – solange für den Drucker nicht ein anderes Drucksystem spezifiziert wird.

Beispiel:

```
[global]
    printing = cups
    printcap name = cups
    load printers = yes
[printers]
   comment = Alle Drucker
   path = /var/spool/samba
   public = yes
   guest ok = yes
   writable = no
```

```
   printable = yes
   printer admin = root, @ntadmins
[PDF-Printer]
   printing = bsd
   comment = PDF creator
   path = /var/tmp
   printable = Yes
   print command = /usr/bin/smbprngenpdf -J '%J' -c %c -s %s -u '%u' -z %z
   create mask = 0600
```

Wie Sie sehen, definieren wir zwar in der [global]-Sektion mit 'printing = cups' und 'load printers = yes' eine Einstellung definieren. (((voriger Abschnitt unverständlich))) Dies bewirkt, dass wie bisher alle CUPS-Drucker von Samba automatisch gefunden und verwendet werden. Für diese Drucker braucht Samba kein 'print command'. Darüber hinaus definieren wir eine spezielle Druckerfreigabe namens 'PDF-Printer'. Für diese verwenden wir einen selbst-gestrickten Druckbefehl, den wir Samba auch mitteilen. ('smbprngenpdf' ist ein Bash-Script, das in neueren SuSE-Versionen integriert ist. Es setzt das Utility **ps2pdf** von Ghostscript ein, um PDFs aus PostScript zu generieren. Sie können mit demselben Mechanismus jederzeit ihre eigenen Skripte in das CUPS-/Samba-System einbinden).

18.17.13 'cups options = ...'

Dieser neue Paramter wird nur wirksam, wenn zugleich 'printing = cups' (für dieselbe Druckfreigabe) gesetzt ist. 'cups options' ist ebenfalls ein service level Parameter. (((auszeichnen?)))

Sein Wert kann einer beliebigen Kombination von Druckoptionen bestehen. Diese Optionen übergibt Samba direkt an CUPS. Sie dürfen beliebige Optionen aus dem CUPS-Anwenderhandbuch verwenden, oder druckerspezifische, die in der Drucker-PPD definiert sind. Die druckerspezifischen Optionen verrät Ihnen z.B. der Befehl 'lpoptins -p druckername -l' (gilt nicht für 'raw'-Drucker).

Ein Anwendungsfall könnte auch darin bestehen, dass Sie allen Druckjobs eine IPP-Option mitgeben, z.B. 'job-hold-until=indefinite'. Diese bewirkt, dass der Job innerhalb des CUPS-Spoolers auf 'Warten' gesetzt wird, bis eine manuelle Freigabe (z.B. über das CUPS-Webinterface) erfolgt.

Eins andere Möglichkeit: eine Kopfseite ('banner page') die für jeden Anwender unterschiedlich ist und der schnelleren Identifikation der eigenen Druckjobs dient.

Beispiele:

```
[global]
    printing = cups
    printcap name = cups
    load printers = yes
[printers]
```

```
   comment = Alle Drucker
   path = /var/spool/samba
   public = yes
   guest ok = yes
   writable = no
   printable = yes
   printer admin = root, @ntadmins
[Teurer_Farblaser]
   cups options = 'job-hold-until=indefinite'
[Abteilungsdrucker_1]
   cups options = 'job-sheets=none,%$USER-banner'
```

Wie Sie sehen, verwendet der 'Abteilungsdrucker_1' eine Kopfseite, deren Name '%$USER' enthält. Das '%$' veranlasst Samba, nach der Umgebungsvariable '$USER' zu suchen, diese zu expandieren und zu ersetzen. Falls der momentane Anwender 'kpfeifle' heisst, wird dem Job also der Befehl '-o job-sheets=none,kpfeifle-banner' mitgegeben. Sie müsen lediglich dafür sorgen, dass auf Seiten von CUPS nun auch tatsächlich eine Datei namens 'kpfeifle-banner' in '/usr/share/cups/banners/' liegt und druckbar ist....

WICHTIG

Bei Verwendung bestimmter Windows-Treiber-Typen (v.a. bei nicht-PostScript-Treibern) müssen (((wer erlaubt ?))) weiterhin in der CUPS-Konfiguration das Drucken 'unbekannter Dateiformate' (also was CUPS als 'application/octet-stream' bezeichnet) erlauben. Sehen Sie hierzu in '/etc/cups/mime.convs' und '/etc/cups/mime.types' nach und entfernen Sie von den entsprechenden Zeilen am Dateiende die Kommentarzeichen. Eine Angabe von 'cups options = raw' in der `smb.conf` alleine reicht hierfür nicht aus!

18.17.14 'printcap cache time = ...,'

Dieser Parameter steuert, wie häufig Samba die Datei `printcap` einliest, um nachzuschauen, ob sich in der Druckerliste Änderungen ergeben haben. Die Voreinstellung ist 'printcap cache time = 0'. Sie verhindert, dass Samba zur Laufzeit die printcap neu einliest. Ein CUPS neu hinzugefügter Drucker ist somit für Samba nicht sofort nutzbar. Wollen Sie diesen trotzdem 'sehen' und nutzen (ohne Samba komplett neu starten zu wollen), müssen Sie allen smbd-Prozessen ein 'HUP'-Signal schicken: 'kill -HUP ‘pidof smbd‘'.

Um eine fortlaufende automatische Aktualisierung der Samba-Druckerliste zu erzwingen,sollten Sie einen Wert in Sekunden eintragen, etwa 'printcap cache time = 60'. Damit stellen Sie sicher, dass alle neuen CUPS-Drucker nach spätestens 1 Minute in Samba ebenfalls sichtbar sind.

18.17.15 'rpcclient setprintername'

Dieses neue 'rpcclient' Sub-Kommando verleiht einem Unix-Drucker einen neuen Künstlernamen für seinen Auftritt in der Windows-Welt.

Dies ist z.B. dann nützlich, wenn Sie Ihren Anwender künftig mit einem Samba-Printserver dienen wollen, ohne sie von den gewohnten Windows-Namen für Drucker (die unter Umständen Leerzeichen enthalten können) entwöhnen zu müssen.

18.17.16 'cups server = ...'

Dieser neue Parameter erlaubt es Ihnen erstmals, Samba- und CUPS-Server auf zwei verschiedenen Maschinen laufen zu lassen. 'cups server = ...' ist ein Paramter, der nur in der [global]-Sektion auftauchen darf.

Weiterhin können Sie damit verschiedenen 'virtuellen Samba-Daemonsünterschiedliche CUPS-Druckserver zuordnen, etwa nach Arbeitsgruppen getrennt.

Zum Einsatz mit verschiedenen CUPS-Servern für unterschiedliche virtuelle smbd-Prozesse müssen Sie diesen Parameter daher per 'include' in die jeweilige `smb.conf` einbinden. Näheres lesen Sie bitte in den Manual-Seiten der `smb.conf` nach.

18.17.17 'VampireDriverFunctions'

Mit dem 'VampireDriverFunctions' hat ein neues Migrationstool in die Samba-Scriptsammlung Einzug gehalten. Dieses ist aus der Not geboren: der Autor hatte die berufliche Aufgabe, im Kundenauftrag einen Windows-NT-Printserver auf eine stärkere Maschine unter Windows XP Professional (!) zu migrieren.

Kein Problem, sagen Sie? Die Praxis sah anders aus:

- mehr als 300 Drucker
- 108 verschiedene Druckertreiber
- einige Druckermodelle z.T. mehr als 7 Jahre alt
- die Original-Datenträger mit den Treibern für viele Modelle nicht mehr auffindbar
- langwierige Internet-Suche nach den Treibern
- 2 Tage Installationsorgie als Diskjockey mit Disketten und CDs
- am Ende (trotz Überstunden) nur ca. 70 Originaltreiber installiert, Rest nicht auffindbar.

Der Autor nahm sich vor, einer solchen Aufgabe nie wieder unvorbereitet gegenübertreten zu müssen. Er schrieb das Script 'VampireDriverFunctions'. Dieses verwendet Samba's Befehle **rpcclient'**- und smbclient, nebst einigen Unix-Utilities wie 'sed', 'awk', 'sort' 'uniq' und einigen anderen, um von einem bestehenden (Samba- oder Windows-)Printserver die Treiberdateien abzusaugen und in einer Verzeichnisstruktur geordnet abzulegen.

Das Skript funktioniert so gut, dass (in einem anderen Fall) die ähnlich grosse Aufgabe, 78 Druckertreiber von einem Server auf einen anderen zu übertragen, bereits nach 23 Minuten

erledigt war. (Dieses Mal ging die Migration allerdings nicht von WinNT nach WinXP, sondern Richtung Linux/Samba ;-))

'VampireDriverFunctions' selbst ist modular aufgebaut und in verschiedene Funktionen gegliedert.

Bedenken Sie, dass 'VampireDriverFunctions' nicht die Druckerwarteschlangen installiert. Diese müssen nach wie vor mit Hilfe des CUPS-'lpadmin'-Befehls (oder entsprechend anderen Methoden) angelegt werden. Auch ordnet das Skript keine der frisch installierten Windows-Treiber den entsprechenden CUPS-Druckerwarteschlangen zu. Dies bleibt einer Serie von 'rpcclient ...setdriver...'-Befehlen vorbehalten. Allerdings ist dies selbst bei einer Zahl von mehr als hundert Druckern innerhalb von 2 Stunden erledigt, wenn erstmal die Treiber in der [print$]-Share bevorratet sind.

'VampireDriverFunctions' ist selbstdokumentierend. Starten Sie es mit dem Befehl 'source VampireDriverFunctions' in einer Bash-Shell. Die Shell liest jetzt die beinhalteten Funktionen ein und listet sie auf:

```
   NOTE: run the listed functions in the same order as listed below.
EXAMPLE: "knoppix@ttyp6[knoppix]$ helpwithvampiredrivers"

   HELP: the "--help" parameter prints usage hints regarding a function.
EXAMPLE: "knoppix@ttyp6[knoppix]$ fetchenumdrivers3listfromNThost --help"

function vampiredrivers_readme()
function enumallfunctions()
function helpwithvampiredrivers()
function fetchenumdrivers3listfromNThost()  # repeat, if no success at first
function createdrivernamelist()
function createprinterlistwithUNCnames()    # repeat, if no success at first
function createmapofprinterstodrivers()
function splitenumdrivers3list()
function makesubdirsforW32X86driverlist()
  function splitW32X86fileintoindividualdriverfiles()
  function fetchallW32X86driverfiles()
  function uploadallW32X86drivers()
function makesubdirsforWIN40driverlist()
  function splitWIN40fileintoindividualdriverfiles()
  function fetchallWIN40driverfiles()
  function uploadallWIN40drivers()
```

Jede dieser Funktionen zeigt Ihnen an, wie sie zu benutzen ist und welche Voraussetzungen Sie schaffen müssen, damit Sie sie erfolgreich ausführen können. Um z.B. die Hilfe für die Funktion 'createdrivernamelist()' zu sehen, geben Sie bitte 'createdrivernamelist –help' ein. Führen Sie jedoch bitte zuerst den Befehl 'vampiredrivers_readme' aus.

Dabei werden Sie erfahren, dass das Script 6 zusätzliche Parameter einlesen muss: die beiden Rechnernamen (Quelle und Ziel), sowie die beiden Benutzernamen und die Passwörter. Als Variablen sind diese mit $nthost, $ntprinteradmin und $ntadminpasswd (für den

Quellrechner) sowie $smbhost, $smbprinteradmin und $smbadminpasswd (für den Zielrechner) bezeichnet. (Anmerkung: auf dem 'Zielrechner' brauchen Sie Rechte als 'Druck-Administrator').

'fetchenumdrivers3listfromNThost'. Diese Funktion holt erstmal eine komplette Liste aller auf dem Quellserver vorrätigen Treiber samt der zugehörigen Treiberdateien. (Achtung, eventuell müssen Sie diese Funktion mehrmals ausführen, da des öfteren die erste Verbindungsaufnahme zum Quellrechner nicht klappt). Diese Liste wird lokal als Datei `$nthost/enumdrivers3list` abgespeichert.

'createdrivernamelist'. Die nächste Funktion ist eine Hilfsfunktion. Sie arbeitet auf der soeben gewonnenen Datei mit den Treiberinformationen des Quellservers. Sie extrahiert aus diese Informationen eine Treibernamens-List.

'splitenumdrivers3list'. Eine weitere Hilfsfunktion zerlegt die Komplettliste in separate Teile für 'Version 2' und 'Version 3' Treiber.

'makesubdirsforW32X86driverlist'. Dieser Schritt legt für jeden Treiber und jede Version ('2' oder '3') ein eigenes Unterverzeichnis an, und zwar unterhalb des aktuellen Arbeitsverzeichnisses..

'splitW32X86fileintoindividualdriverfiles' Hier wird pro Treiber eine Liste aller zugehörigen Dateien angelegt mitsamt den 'UNC-Pfaden', wo sie auf dem Quellserver gespeichert sind.

'fetchallW32X86driverfiles'. Jetzt wird es wieder Ernst: anhand der zuvor geschaffenene Listen, holt dieses Funktion jetzt mittels smbclient die einzelnen Treiberdateien ab und speichert sie erstmal in der lokalen Verzeichnisstruktur ab.

'uploadallW32X86drivers'. Zuletzt werden die zuvor gewonnenen Treiberdateien auf den Zielserver hochgeladen. Für die Datenübertragung kommt wieder smbclient zum Einsatz, die Ernennung zu richtigen Windowstreibern nimmt abschliessend **rpcclient** vor.

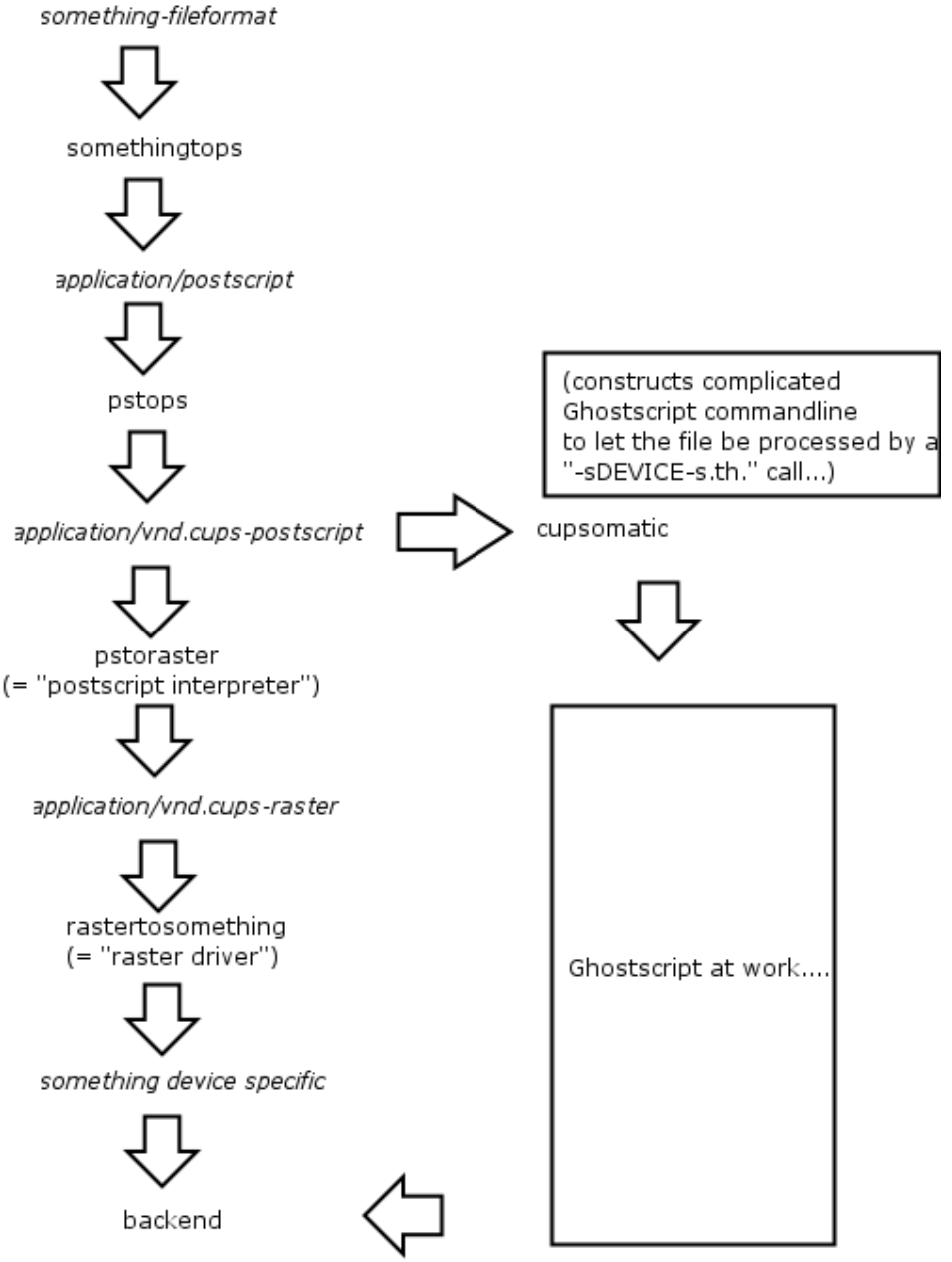
Für die Treiber der 'WIN40'-Architektur (also für Win95/98/ME) sind anologe Funktionen vorhanden.

Wenn Sie die aufgelisteten Funktionen jetzt nacheinander manuell ausführen, holen Sie die Treiber von einem Server A (Samba oder Windows, in dem Skript allerdings immer als '$nthost' bezeichnet) und laden diese Anschliessend auf Server B (Samba oder Windows, im Skript jeweils '$smbhost') hoch. Sie können dies leicht in einem sehr einfachen Skript automatisieren. Dieses muss zuerst die 'VampireDriverFunctions' einlesen ('sourcen') sowie die Parameter für Quell- und Ziel-Rechner und anschliessend einfach die betreffenden Funktionen nacheinander aufrufen::

```
#!/bin/bash

$nthost="10.11.12.13"            # adapt to your own environment
$ntprinteradmin=Administrator    # adapt to your own environment
$ntadminpasswd=secret            # adapt to your own environment

$smbhost="samba.localdomain.de"  # adapt to your own environment
$smbprinteradmin=root            # adapt to your own environment
$smbdminpasswd=topsecret         # adapt to your own environment

source VampireDriverFunctions

fetchenumdrivers3listfromNThost  # repeat, if no success at first
createdrivernamelist
createprinterlistwithUNCnames    # repeat, if no success at first
createmapofprinterstodrivers
splitenumdrivers3list
makesubdirsforW32X86driverlist
splitW32X86fileintoindividualdriverfiles
fetchallW32X86driverfiles
uploadallW32X86drivers
```

Die Knoppix-CD beinhaltet seit der Release 3.4 (CeBIT 2004) eine funktionierende Vorläufer-Version dieses Scripts. Es trägt hier allerdings den Namen 'print-utils-get-functions.sh'. Sie können dieses Tool auch von der laufenden Knoppix-CD aus benutzen, sollten dabei allerdings genügend Hauptspeider haben, um die Treiber zeitweilig in der RAM-Disk speichern zu können (oder ein 'permanentes Homeverzeichnis für den Benutzer Knoppix' auf der Festplatte einrichten).

'VampireDriverFunctions' finden Sie im Verzeichnis 'examples/printing/' der Samba-Quellen.



Note, that cupsomatic "kidnaps" the printfile after the application/vnd.cups-postscript stage and deviates it gh the CUPS-external, systemwide Ghostscript installation, bypassing the "pstoraster" filter (therefore also bypassing the CUPS-raster-drivers "rastertosomething", and hands the rasterized file directly to the CUPS backend...

cupsomatic is not made by the CUPS developers. It is an independent contribution to printing development, made by people from Linuxprinting.org. (see also http://www.cups.org/cups-help.html)

Figure 18.17. Filterkette mit cupsomatic

Kapitel 19

STAPELBARE VFS-MODULE

19.1 Eigenschaften und Vorzüge

Seit Samba-3 gibt es eine Unterstützung für stapelbare VFS-(Virtual File System-)Module. Samba gibt jede Anfrage an das UNIX-Filesystem durch das geladene VFS-Modul weiter. Dieses Kapitel deckt alle Module aus den Samba-Quellen ab und nennt einige Referenzen auf externe Module.

19.2 Beschreibung

Sind die verteilten Bibliotheken nicht bereits im binären Paket Ihrer Plattform enthalten, könnte es Probleme beim Kompilieren geben, da diese auf verschiedenen Plattformen verschieden kompiliert und verlinkt werden. Momentan wurden diese auf GNU/LINUX und IRIX getestet.

Um die VFS-Module benutzen zu können, erstellen Sie eine Freigabe ähnlich der unten gezeigten. Der essenzielle Parameter ist der vfs objects-Parameter, bei dem man einen oder mehrere VFS-Module als Namen angeben kann. Beispiel **??** zeigt, wie Sie Beispiel, um alle Zugriffe auf Dateien loggen und gelöschte Dateien in einen Papierkorb werfen können.

Beispiel 19.2.1. smb.conf mit VFS-Modulen

```
[audit]
        comment = Überwachter /Daten-Ordner
        path = /data
        vfs objects = audit recycle
        writeable = yes
        browseable = yes
```

Die Module werden in der Reihenfolge benutzt, in der sie angegeben sind. Nehmen wir an, Sie möchten ein Virus-Scanner-Modul und ein Papierkorb-Modul haben. Es wäre schlauer, das Viren-Scanner-Modul als erstes Modul festzulegen, sodass es eventuelle Viren sofort entdeckt, bevor die Datei von jemand anderem benutzt wird. Die Einstellung ist dann: vfs objects = vscan-clamav recycle.

Samba wird versuchen, Module vom `/lib`-Ordner des Stammverzeichnisses der Samba-Installation zu laden (normalerweise `/usr/lib/samba/vfs` oder `/usr/local/samba/lib/vfs`).

Manche Module können auch zweimal für die gleiche Freigabe verwendet werden. Dazu verwenden Sie eine Konfiguration ähnlich der aus Beispiel **??**.

Beispiel 19.2.2. smb.conf mit mehreren VFS-Modulen

```
[test]
        comment = VFS TEST
        path = /data
        writeable = yes
        browseable = yes
        vfs objects = Beispiel:Beispiel1 Beispiel Beispiel:test
        Beispiel1: parameter = 1
        Beispiel: parameter = 5
        test: parameter = 7
```

19.3 Enthaltene Module

19.3.1 audit

Ein einfaches Modul, um Dateioperationen im syslog aufzuzeichnen. Folgende Operationen werden aufgezeichnet:

- Freigabe verbinden/trennen
- Ordner öffnen/erstellen/löschen
- Datei öffnen/schließen/umbenennen/unlink/chmod

19.3.2 extd_audit

Dieses Modul ist identisch mit dem **audit**-Modul, außer dass es sowohl ins syslog als auch in die **smbd**-Log-Dateien schreibt. Der Log-Level für dieses Modul wird in der `smb.conf`-Datei gesetzt.

Gültige Einstellungen und Informationen darüber, was alles aufgezeichnet wird, sind in Tabelle **??** zu finden.

19.3.3 fake_perms

Dieses Modul wurde erstellt, um Roaming-Profil-Dateien und -Ordner (auf dem Samba-Server unter UNIX) als nur lesbar zu setzen. Dieses Modul - sollte es unter der Profiles-Freigabe installiert sein - gibt dem Client an, dass er Profil-Ordner und Dateien beschreiben

Tabelle 19.1. Ausführliche Beschreibung der Log-Informationen

Log Level	Log Details - Ordner- und Dateioperationen
0	Erstellen / Löschen
1	Erstellen / Löschen / Umbenennen / Berechtigungen ändern
2	Erstellen / Löschen / Umbenennen / Berechtigungen ändern / Öffnen / Schließen

darf. Das genügt dem Client, auch wenn die Dateien nicht überschrieben werden, falls er sich abmeldet oder herunterfährt.

19.3.4 recycle

Ein dem Papierkorb ähnliches Modul. Wird es benutzt, werden Lösch-(UNLINK-)Befehle abgefangen, und die Datei wird in den recycle-Ordner verschoben, anstatt gelöscht zu werden. Das ist im Prinzip dieselbe Funktion, die der Ordner **Papierkorb** auf Windows-Computern erfüllt.

Der **Papierkorb** wird weder in Windows Explorer-Ansichten der Freigabe noch in den Netzwerkverbindungen erscheinen. Es wird automatisch ein `.recycle`-Ordner erstellt, sobald eine Datei gelöscht wird. Benutzer können Dateien vom `.recycle`-Ordner wiederherstellen. Falls der *recycle:keeptree*-Parameter gesetzt wurde, können gelöschte Dateien unter dem gleichen Pfad gefunden werden, in dem sie vor dem Löschen waren.

Folgende Optionen werden für das **recycle**-Modul unterstützt:

recycle:repository Relativer Pfad des Ordners, in dem gelöschte Dateien abgelegt werden sollen.

recycle:keeptree Legt fest, ob die Ordnerstruktur beibehalten werden soll oder ob die Dateien des gelöschten Ordners getrennt im Papierkorb aufbewart werden sollen.

recycle:versions Ist diese Option gesetzt, werden zwei Dateien mit dem gleichen Namen im Papierkorb aufbewahrt. Die neuere Version der Datei wird in „*Copy #x of Dateiname*“ umbenannt.

recycle:touch Legt fest, ob das Datum des letzten Zugriffs verändert werden soll, wenn die Datei in den Papierkorb kommt.

recycle:maxsize Dateien, die größer sind als die in diesem Parameter festgelegte Größe in Bytes, werden nicht in den Papierkorb verschoben.

recycle:exclude Auflistung der Dateien, die nicht in den Papierkorb verschoben, sondern normal gelöscht werden sollen.

recycle:exclude_dir Enthält eine Liste von Ordnern. Falls Dateien aus diesen Ordnern gelöscht werden, werden sie nicht in den Papierkorb verschoben, sondern normal gelöscht.

recycle:noversions Das Gegenteil des *recycle:versions*-Parameters. Falls beide Optionen gesetzt sind, wird *recycle:noversions* verwendet.

19.3.5 netatalk

Das netatalk-Modul erleichtert die Koexistenz von Samba und netatalk-Dateifreigabe-Diensten.

Es hat folgende Vorteile gegenüber dem alten netatalk-Modul:

- Es schert sich nicht um das Erstellen von „*.AppleDouble*“-Forks, sondern hält sie nur synchron.
- Falls eine Freigabe in der `smb.conf` kein „*.AppleDouble*“-Objekt in der „*hite*“- oder „*veto*“-Liste enthält, wird es automatisch hinzugefügt.

19.4 Anderweitig verfügbare VFS-Module

Dieser Abschnitt enthält eine Auflistung verschiedener anderer VFS-Module, die es gibt, die aber aus verschiedenen Gründen nicht im CVS- Baum von Samba enthalten sind (z.B. da es für die Entwickler leichter ist, einen eigenen CVS-Baum zu pflegen.)

Die Auflistung der Module hier soll keine Bewertung der Stabilität oder Funktionalität sein.

19.4.1 DatabaseFS

URL: <`http://www.css.tayloru.edu/~elorimer/databasefs/index.php`>

Von Eric Lorimer. <`mailto:elorimer@css.tayloru.edu`>

Ich habe ein VFS-Modul entworfen, das einem Read-only-Dateisystem gleichkommt. Es gibt die Informationen einer Datenbank in einer modularen und generischen Weise als ein Dateisystem aus, um die Benutzung verschiedener Datenbanken zu ermöglichen. (es wurde ursprünglich dazu entworfen, MP3s in Ordnern wie „*Künstler*“, „*Lied-Stichwörter*“ usw. zu organisieren. Ich habe es aber auch schon für ein Studenten-Register benutzt). Die Ordnerstruktur wird in der Datenbank gespeichert, und das Modul schert sich nicht um die Datenbankstruktur außerhalb der Tabelle, die es braucht.

Ich wäre dankbar für Rückmeldungen jeder Art: Kommentare, Vorschläge, Patches usw. Ich hoffe, dass es sich als brauchbar für jemanden erweist, der ein virtuelles Dateisystem erstellen möchte.

19.4.2 vscan

URL: <http://www.openantivirus.org/>

`samba-vscan` ist ein „*Proof-of-concept*“-Modul für Samba, das die VFS-Funktion (Virtual File System) von Samba 2.2.x/3.0 alphaX nutzt. Natürlich muss Samba mit VFS-Unterstützung kompiliert werden. `samba-vscan` unterstützt viele Virenscanner und wird von Rainer Link gepflegt.

Kapitel 20

WINBIND: BENUTZUNG VON DOMÄNENKONTEN

20.1 Eigenschaften und Vorzüge

Die Integration von UNIX und Microsoft Windows NT durch eine einheitliche Anmeldung („*unified logon*“) galt lange Zeit als „*heiliger Gral*“ in heterogenen EDV-Umgebungen.

Es gibt eine weitere Sache, ohne die die UNIX- und Microsoft Windows-Netzwerk-Interoperabilität leiden würde. Es ist zwingend notwendig, dass es einen Mechanismus gibt, mit dem es möglich ist, Dateien über UNIX-Systeme hinweg bereitzustellen und gleichzeitig die Integrität der Domänen-Benutzer- und Gruppenrechte zu wahren.

winbind ist ein Bestandteil der Samba-Suite, der das Problem der einheitlichen Anmeldung löst. Winbind benutzt eine UNIX-Implementierung der Microsoft RPC-Aufrufe, „*Pluggable Authentication*“-Module (PAM) und den Name Service Switch (NSS), um Windows NT-Domänenbenutzer auf UNIX-Systemen als UNIX-Benutzer erscheinen und arbeiten zu lassen. Dieses Kapitel beschreibt das System von winbind, erklärt die Funktionsweise und zeigt, wie es konfiguriert wird und wie es intern arbeitet.

Winbind stellt drei unterschiedliche Funktionen zur Verfügung:

- Die Authentifizierung der Benutzerbeglaubigung (mittels PAM)
- Die Auflösung der Identität (mittels NSS)
- Winbind hält eine Datenbank namens winbind_idmap.tdb, in der die Zuordnungen zwischen den UNIX UIDs/GIDs und den NT-SIDs vermerkt sind. Diese Zuordnungen werden nur für Benutzer und Gruppen verwendet, die nicht über eine lokale UID/GID verfügen. Winbind sichert die Zusammengehörigkeit zwischen der UID/GID, die im idmap-uid/gid-Bereich zugeteilt wird, und der NT-SID. Wenn *idmap backend* auf den Wert „*ldapsam:url*“ statt für die Nutzung einer lokalen Datei gesetzt ist, dann holt Winbind diese Informationen aus der LDAP-Datenbank.

ANMERKUNG

Wenn **winbindd** nicht läuft, dann wird der smbd (der **winbindd** aufruft) auf die nur lokal vorhandenen Informationen der `/etc/passwd` und `/etc/group` ohne eine dynamische Zuordnung zurückgreifen.

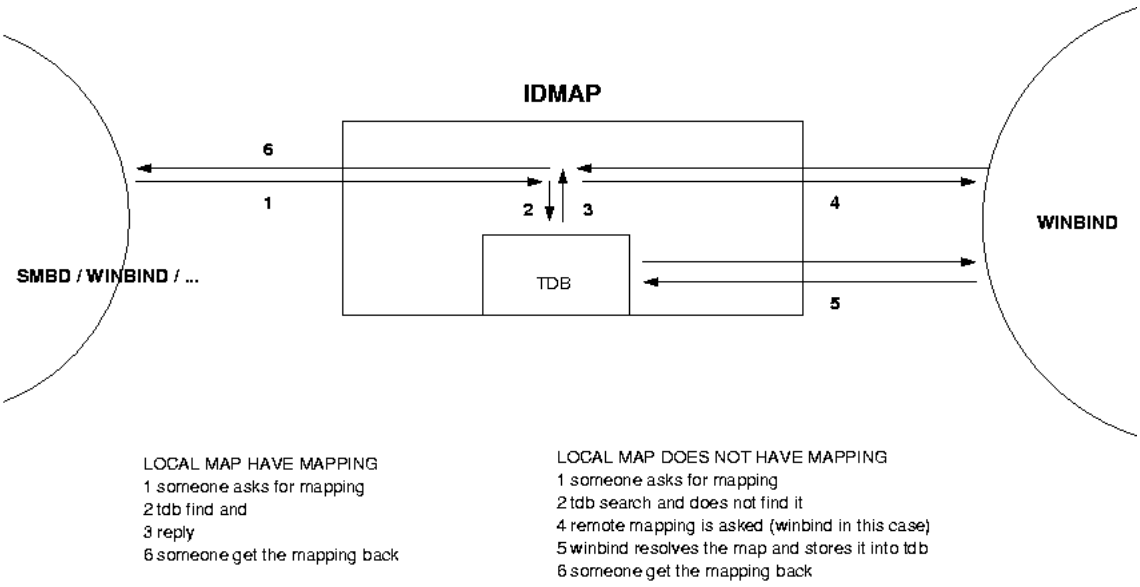


Figure 20.1. Winbind Idmap

20.2 Einführung

Es ist allgemein bekannt, dass UNIX und Windows NT verschiedene Modelle zur Repräsentation von Benutzer- und Gruppen-Informationen haben und verschiedene Technologien nutzen, um diese zu implementieren. Diese Tatsache macht es schwierig, die beiden Systeme auf befriedigende Weise zu integrieren.

Eine gängige Lösung ist es, identisch benannte Benutzerkonten sowohl im Windows- als auch im UNIX-System anzulegen und die Samba-Suite dafür zu nutzen, Datei- und Druckdienste zwischen den beiden Systemen anzubieten. Diese Lösung ist jedoch weit davon entfernt, perfekt zu sein, da das Hinzufügen und Löschen von Benutzern auf beiden Gruppen von Maschinen zur lästigen Pflicht wird und zwei Sätze Passwörter benötigt werden. Beides führt zu Synchronisationsproblemen zwischen Windows und UNIX und zur Verwirrung der Benutzer.

Wir teilen das Problem der einheitlichen Anmeldung für UNIX-Maschinen in drei kleinere Probleme auf:

- Das Beziehen von Windows NT-Benutzer- und Gruppen-Informationen
- Die Authentifikation von Windows NT-Benutzern
- Das Ändern von Passwörtern der Windows NT-Benutzer

Im Idealfall würde eine weitblickende Lösung des „*unified logon*“-Problems alle oben genannten Teilprobleme lösen, ohne Informationen auf den UNIX-Systemen zu duplizieren und ohne zusätzliche Arbeiten für den System-Administrator zu verursachen, wenn er Benutzer und Gruppen auf den einzelnen Systemen administriert. Das Winbind-System bietet eine einfache und elegante Lösung für alle drei Teile des „*unified logon*“-Problems an.

20.3 Was Winbind anbietet

Winbind vereint die UNIX- und Windows NT-Konten-Verwaltung, indem es einer UNIX-Maschine erlaubt, ein vollwertiges Mitglied einer NT-Domäne zu werden. Sobald dies erfolgt ist, sieht die UNIX-Maschine die NT-Benutzer und -Gruppen so, als ob sie „*native*“ UNIX-Benutzer und -Gruppen wären, was die Benutzung der NT-Domäne in fast derselben Art erlaubt, wie NIS+ in reinen UNIX-Umgebungen verwendet wird.

Als Endergebnis wird, immer wenn ein Programm auf der UNIX-Maschine das Betriebssystem nach einem Benutzer- oder Gruppen-Namen fragt, die Anfrage an den NT-Domänencontroller weitergegeben, der diese Namensabfrage durchführt. Weil Winbind sich auf einem sehr tiefgreifenden Level ins Betriebssystem einhängt (über die NSS-Namensauflösungsmodule in der C-Library), ist diese Umleitung zum NT-Domänencontroller völlig transparent.

Die Benutzer auf der UNIX-Maschine können dann NT-Benutzer- und NT-Gruppen-Namen so verwenden, als ob sie „*native*“ UNIX-Namen wären. Sie können mit chown Eigentümer von Dateien werden, so dass die Dateien NT-Domänen-Benutzern gehören, oder sich sogar auf einer UNIX-Maschine anmelden und eine UNIX-X-Window-Session als Domänen-Benutzer ausführen.

Das einzige sichtbare Anzeichen, dass Winbind verwendet wird, ist, dass Benutzer- und Gruppen-Namen die Form `DOMÄNE\benutzer` und `DOMÄNE\gruppe` annehmen. Das ist notwendig, da Winbind auf diese Weise erkennt, wann eine Umleitung zum Domänencontroller erforderlich ist und auf welche Domäne sich diese Anfrage bezieht.

Zusätzlich bietet Winbind einen Authentifikationsdienst, der sich ins PAM-System (Pluggable Authentication Modules) einhängt, um allen PAM-fähigen Applikationen die Authentifikation über eine NT-Domäne anzubieten. Diese Fähigkeit löst das Problem der Synchronisation von Passwörtern zwischen Systemen, da alle Passwörter an nur einem Platz gespeichert werden - auf dem Domänencontroller.

20.3.1 Zielgruppen

Winbind zielt auf Organisationen ab, die eine existierende, auf NT-Domänen basierende Infrastruktur haben, in die sie UNIX-Maschinen integrieren wollen. Winbind erlaubt diesen Organisationen, UNIX-Maschinen einzusetzen, ohne eine separate Struktur für deren Konten

aufrechterhalten zu müssen. Dies vereinfacht den administrativen Overhead der Integration von UNIX in einer NT-basierenden Organisation.

Eine weitere interessante Art, in der wir erwarten, dass Winbind eingesetzt wird, ist Winbind als zentraler Teil von UNIX-basierenden Geräten. Solche Geräte, die Datei- und Druck-Dienste für MS-basierende Netzwerke anbieten, können Winbind einsetzen, um eine nahtlose Integration in die Domäne zu erreichen.

20.4 Wie Winbind arbeitet

Das Winbind-System ist rund um eine Client-Server-Architektur entworfen worden. Ein **winbindd**-Daemon mit langer Laufzeit hört auf einem UNIX-Domänen-Socket auf ankommende Anfragen. Diese Anfragen („*Requests*“) werden von den NSS- und PAM-Clients generiert und sequenziell verarbeitet.

Die Technologien, die zur Implementation von Winbind verwendet werden, werden nachfolgend im Detail beschrieben.

20.4.1 Microsoft Remote Procedure Calls

In den letzten paar Jahren wurden von verschiedenen Samba-Team-Mitgliedern Anstrengungen unternommen, die verschiedenen Aspekte des Systems „*Microsoft Remote Procedure Call*“ (MSRPC) zu entschlüsseln. Dieses System wird für die meisten netzwerkbasierenden Operationen zwischen Windows NT-Maschinen verwendet, inklusive Fernwartung, Benutzer-Authentifikation und Druck-Spooling. Obwohl diese Arbeit ursprünglich zur Unterstützung der Funktionalitäten primären Domänencontroller (PDC) in Samba geleistet wurde, hat sie auch eine Menge Code hervorgebracht, die für andere Zwecke eingesetzt werden kann.

Winbind verwendet verschiedene MSRPC-Aufrufe, um Domänen-Benutzer und -Gruppen aufzuzählen und detaillierte Informationen über einzelne Benutzer oder Gruppen zu beziehen. Andere MSRPC-Aufrufe können zur Authentifikation von NT-Domänen-Benutzern verwendet werden und zum Ändern von Benutzer-Passwörtern. Durch direktes Abfragen eines Windows-PDCs stellt Winbind die Zuordnung von NT-Konteninformationen zu UNIX-Benutzer- und Gruppen-Namen her.

20.4.2 Microsoft Active Directory

Seit Ende 2001 hat Samba die Fähigkeiten, mit Microsoft Windows 2000 über dessen „*Native Mode*“-Protokolle zusammenzuarbeiten statt über die NT4-RPC-Dienste. Unter Verwendung von LDAP und Kerberos kann ein Domänen-Mitglied, das Winbind ausführt, Benutzer und Gruppen genau in derselben Art aufzählen, wie es ein Windows 200x-Client tun würde, und schafft damit eine viel effizientere und effektivere Winbind-Implementation.

20.4.3 Name Service Switch

Der Name Service Switch (NSS) ist eine Funktionalität, die in vielen UNIX-Betriebssystemen vorhanden ist. Er erlaubt das Auflösen von System-Informationen, wie Hostnamen, Mail-Aliases oder Benutzerinformationen unter Verwendung verschiedener Quellen. Zum Beispiel kann eine Standalone-UNIX-Workstation ihre Systeminformationen aus einer Reihe von einfachen Dateien im lokalen Dateisystem beziehen. Eine vernetzte Workstation könnte zuerst versuchen, die Systeminformationen aus den lokalen Dateien zu beziehen und dann eine NIS-Datenbank oder einen DNS-Server nach Informationen zu Hostnamen befragen.

Die NSS-API erlaubt es Winbind, sich selbst als Quelle für Systeminformationen anzubieten, wenn UNIX-Benutzer- und Gruppen-Namen aufgelöst werden sollen. Winbind verwendet dieses Interface und Informationen, die mit MSRPC-Aufrufen von einem Windows NT-Server bezogen wurden, um eine neue Informationsquelle zur Verfügung zu stellen. Unter Verwendung von Standard-UNIX-Bibliotheksaufrufen kann man die Benutzer und Gruppen auf einer UNIX-Maschine, die Winbind ausführt, auflisten und alle Benutzer und Gruppen in einer NT-Domäne plus diejenigen jeglicher Vertrauensdomänen so sehen, als ob sie lokale Benutzer und Gruppen wären.

Die primäre Steuerdatei für NSS ist `/etc/nsswitch.conf`. Wenn eine UNIX-Applikation eine Anfrage stellt, durchsucht die C-Library `/etc/nsswitch.conf` nach einer Zeile, die dem erfragten Dienst entspricht, z.B. dem Dienst „*passwd*“, der verwendet wird, wenn nach Benutzer- oder Gruppen-Namen gesucht wird. Diese Konfigurationszeile gibt an, welche Implementation dieses Diensts in welcher Reihenfolge versucht werden soll. Wenn die Zeile

```
passwd: files example
```

lautet, dann wird die C-Library zuerst ein Modul namens `/lib/libnss_files.so` laden, gefolgt vom Modul `/lib/libnss_example.so`. Die C-Library wird dynamisch jedes dieser Module der Reihe nach laden und die Auflösungsfunktionen innerhalb jedes Moduls ausführen, um zu versuchen, die Anfrage aufzulösen. Sobald dies geschehen ist, gibt die C-Library das Ergebnis an die Anwendung zurück.

Dieses NSS-Interface bietet eine einfache Möglichkeit, Winbind in das Betriebssystem einzuhängen. Sie müssen nur `libnss_winbind.so` in `/lib/` platzieren und dann „*winbind*“ an der richtigen Stelle in `/etc/nsswitch.conf` hinzufügen. Die C-Library wird dann Winbind zur Namensauflösung aufrufen.

20.4.4 Pluggable Authentication Modules

Pluggable Authentication Modules, auch als PAM bekannt, sind ein System zum Abstrahieren von Authentifikations- und Autorisationstechnologien. Mit einem PAM-Modul ist es möglich, verschiedene Authentifikationsmethoden für verschiedene Systemanwendungen zu spezifizieren, ohne diese Anwendungen neu kompilieren zu müssen. PAM ist außerdem beim Implementieren einer speziellen Richtlinie für die Autorisierung hilfreich. Zum Beispiel könnte ein System-Administrator Konsolen-Logins nur den Benutzern erlauben, die in der lokalen Passwort-Datei gespeichert sind, und Netzwerk-Logins nur dem Benutzern, die in einer NIS-Datenbank gespeichert sind.

Winbind nutzt das Authentifikationsmanagement- und Passwort-Management-PAM-Interface, um Windows-NT-Benutzer in ein UNIX-System zu integrieren. Das erlaubt es Windows-NT-Benutzern, sich an einer UNIX-Maschine anzumelden und durch einen passenden PDC authentifiziert zu werden. Diese Benutzer können außerdem ihre Passwörter ändern, und diese Veränderung findet direkt auf dem PDC statt.

PAM wird dadurch konfiguriert, dass im Verzeichnis `/etc/pam.d/` Steuerdateien für jeden Dienst bereitgestellt werden, der Authentifikation benötigt. Wenn eine Authentifikationsanfrage von einer Anwendung gestellt wird, liest der PAM-Code in der C-Library aus dieser Steuerdatei, welche Module in welcher Reihenfolge für diese Authentifikation geladen werden müssen. Das Interface vereinfacht das Hinzufügen neuer Authentifikationsdienste zu Winbind. Sie müssen lediglich das Modul `pam_winbind.so` in das Verzeichnis `/lib/security/` kopieren und die Steuerdateien der relevanten Dienste aktualisieren, um eine Authentifikation via Winbind zu erlauben. Lesen Sie die PAM-Dokumentation in Kapitel **??** „PAM-basierte verteilte Authentifizierung“ für mehr Informationen dazu.

20.4.5 Zuordnung von Benutzer- und Gruppen-IDs

Wenn ein Benutzer oder eine Gruppe unter Windows NT/200x angelegt wird, wird ihm bzw. ihr ein „*numerical relative identifier*“ (RID) zugeordnet. Das ist etwas anders als in UNIX, das einen Nummernbereich für Benutzer und denselben Nummernbereich für Gruppen hat. Es ist die Aufgabe von Winbind, die RIDs in UNIX-IDs zu konvertieren und vice versa. Wenn Winbind konfiguriert wird, wird ihm ein Teil des UNIX-Benutzer-ID-Namensraums und ein Teil des UNIX-Gruppen-ID-Namensraums zugewiesen, um darin die Windows NT-Benutzer und -Gruppen zu speichern. Wenn ein Windows NT-Benutzer zum ersten Mal aufgelöst werden soll, wird ihm die nächste freie UNIX-ID aus dem Bereich zugewiesen. Derselbe Prozess wird für Windows NT-Gruppen angewendet. Im Laufe der Zeit hat Winbind dann alle Windows NT-Benutzer und -Gruppen entsprechenden UNIX-Benutzern und -Gruppen zugewiesen.

Die Ergebnisse dieser Zuordnung werden dauerhaft in einer ID-Zuordnungsdatenbank abgelegt (gespeichert in einer tdb-Datenbank). Das gewährleistet die konsistente Zuordnung von RIDs zu UNIX-IDs.

20.4.6 Das Cachen der Resultate

Ein aktives System kann sehr viele Anfragen nach Benutzer- und Gruppen-Namen generieren. Um die Netzwerklast dieser Anfragen zu reduzieren, verwendet Winbind ein Caching-Schema, das auf der SAM-Sequenznummer beruht, die von NT-Domänencontrollern zur Verfügung gestellt wird. Benutzer- oder Gruppen-Informationen, die von einem PDC zurückgegeben werden, werden von Winbind gemeinsam mit einer auch vom PDC vergebenen Sequenznummer gepuffert. Diese Sequenznummer wird immer dann von Windows NT erhöht, wenn irgendeine Benutzer- und Gruppen-Information verändert wird. Wenn ein gepufferter Eintrag veraltet ist, wird die Sequenznummer vom PDC abgefragt und mit der Sequenznummer des Cache-Eintrags verglichen. Stimmen die beiden nicht überein, wird die gepufferte Information verworfen und die aktuelle Information direkt vom PDC abgefragt.

20.5 Installation und Konfiguration

20.5.1 Einführung

Dieser Abschnitt beschreibt die Abläufe, die notwendig sind, um Winbind in Betrieb zu nehmen. Winbind kann eine Zugriffs- und Authentifikationsverwaltung für Windows-Domänen-Benutzer zur Verfügung stellen, indem es einen Windows NT- oder Windows 200x-PDC sowohl für normale Dienste wie telnet und ftp als auch für Samba zur Verfügung stellt.

- *Warum sollte ich das tun?*

  Dies erlaubt dem Samba-Administrator, auf dem Authentifikationsmechanismus des Windows NT/200x-PDC für die Authentifikation von Domänen-Mitgliedern aufzubauen. Windows NT/200x-Benutzer müssen nicht länger Konten auf dem Samba-Server haben.

- *Wer sollte dieses Dokument lesen?*

  Dieses Dokument ist für System-Administratoren gedacht. Wenn Sie Samba auf einem Datei-Server implementieren und Sie wollen (ziemlich einfach) bestehende Windows NT/200x-Benutzer von Ihrem PDC auf dem Samba-Server integrieren, ist dieses Dokument das richtige für Sie.

20.5.2 Anforderungen

Wenn Sie eine Samba-Konfigurationsdatei haben, die Sie momentan benutzen, *SICHERN SIE DIE DATEI!* Wenn Ihr System bereits PAM verwendet, *SICHERN SIE* die Inhalte des Verzeichnisses `/etc/pam.d`! Wenn Sie noch keine Bootdiskette angelegt haben, *ERSTELLEN SIE JETZT EINE!*

Das Herumbasteln an den PAM-Konfigurationsdateien kann es nahezu unmöglich machen, sich an Ihrer Maschine anzumelden. Sie müssen imstande sein, im „*single user mode*“ Ihre Maschine neu zu booten und Ihr Verzeichnis `/etc/pam.d` in den Urzustand zu versetzen, wenn Sie von Ihren Fortschritten irgendwie frustriert sein sollten.

Die letzte Version von Samba-3 beinhaltet einen funktionierenden Winbind-Daemon. Bitte besuchen Sie die Samba-Website <`http://samba.org/`>, oder - noch besser - Ihren nächsten Samba-Mirror, um Anleitungen zum Download des Quellcodes zu erhalten.

Um Domänen-Benutzern die Fähigkeit zu verleihen, auf Samba-Freigaben und -Dateien zuzugreifen, wie auch auf möglicherweise andere von Ihrer Samba-Maschine angebotene Dienste, muss PAM auf dieser Maschine ordnungsgemäß eingerichtet sein. Um die Winbind-Module zu kompilieren, sollten Sie zumindest die PAM-Entwickler-Bibliotheken auf Ihrem System installiert haben. Bitte sehen Sie sich dazu auch die PAM-Website <`http://www.kernel.org/pub/linux/libs/pam/`> an.

20.5.3 Testen

Bevor Sie beginnen, ist es möglicherweise das Beste, all die Samba-bezogenen Daemons zu killen, die auf Ihrem Server laufen. Killen Sie all die smbd-, nmbd- und winbindd -Prozesse,

die da laufen. Um PAM zu verwenden, stellen Sie sicher, dass Sie das Standard-PAM-Paket haben, das die Verzeichnis-Struktur `/etc/pam.d` unterstützt, und die PAM-Module enthält, die von PAM-fähigen Diensten verwendet werden, sowie einige PAM-Bibliotheken, und die Einträge für PAM in `/usr/doc` und `/usr/man`. Winbind kann besser in Samba kompiliert werden, wenn auch das Paket „*pam-devel*“ installiert ist. Dieses Paket beinhaltet die Header-Dateien, die zum Kompilieren PAM-fähiger Anwendungen benötigt werden.

20.5.3.1 Konfigurieren Sie nsswitch.conf und die Winbind-Bibliotheken unter Linux und Solaris

PAM ist eine Standard-Komponente der meisten aktuellen UNIX/Linux-Systeme. Leider installieren wenige Systeme die `pam-devel`-Bibliotheken, die benötigt werden, um ein PAM-fähiges Samba zu kompilieren. Zusätzlich kann Samba-3 automatisch die Winbind-Dateien in die benötigten Verzeichnisse auf Ihrem System installieren. Bevor Sie also zu tief graben, prüfen Sie zuerst, ob die nachfolgende Konfiguration wirklich notwendig ist. Es kann sein, dass Sie nur `/etc/nsswitch.conf` konfigurieren müssen.

Die Bibliotheken zur Ausführung des winbindd-Daemons durch nsswitch müssen in die entsprechenden Verzeichnisse kopiert werden:

```
root# cp ../samba/source/nsswitch/libnss_winbind.so /lib
```

Ich habe außerdem herausgefunden, dass der folgende Symlink angelegt werden muss:

```
root# ln -s /lib/libnss_winbind.so /lib/libnss_winbind.so.2
```

Und im Falle von Sun Solaris:

```
root# ln -s /usr/lib/libnss_winbind.so /usr/lib/libnss_winbind.so.1
root# ln -s /usr/lib/libnss_winbind.so /usr/lib/nss_winbind.so.1
root# ln -s /usr/lib/libnss_winbind.so /usr/lib/nss_winbind.so.2
```

Nun müssen Sie als root die Datei `/etc/nsswitch.conf` editieren, um Benutzer- und Gruppen-Einträge vom winbindd-Daemon sichtbar zu machen. Mein Eintrag in `/etc/nsswitch.conf` sieht nach dem Editieren so aus:

```
passwd:     files winbind
shadow:     files
group:      files winbind
```

Die vom Daemon **winbindd** benötigten Bibliotheken werden automatisch in den Cache von **ldconfig** eingetragen, sobald Ihr System das nächste Mal neu startet, aber es geht schneller (und ohne Reboot), wenn Sie das von Hand tun:

```
root#/sbin/ldconfig -v | grep winbind
```

Dies macht `libnss_winbind` für winbindd verfügbar und gibt eine Bestätigung zurück.

20.5.3.2 NSS Winbind auf AIX

(Dieser Abschnitt ist nur für jene gedacht, die AIX betreiben.)

Das Winbind-AIX-Identifikationsmodul wird als `libnss_winbind.so` im nsswitch-Verzeichnis des Samba-Quellcodes kompiliert. Diese Datei kann ins Verzeichnis `/usr/lib/security` kopiert werden, und die AIX-Namenskonvention würde sagen, dass es WINBIND genannt werden sollte. Ein Absatz wie

```
WINBIND:
        program = /usr/lib/security/WINBIND
        options = authonly
```

kann dann zu `/usr/lib/security/methods.cfg` hinzugefügt werden. Dieses Modul unterstützt nur die Identifikation, aber es gibt Meldungen über die erfolgreiche Verwendung des Standard-Winbind-PAM-Moduls für die Authentifikation. Seien Sie mit dem Konfigurieren ladbarer Authentifikationsmodule vorsichtig, da Sie es damit unmöglich machen können, sich am System anzumelden. Mehr Informationen zur AIX-Authentifikationsmodul-API finden Sie unter „*Kernel Extensions and Device Support Programming Concepts for AIX*“. Chapter 18. Loadable Authentication Module Programming Interface <`http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/aixprggd/kernextc/sec_load_mod.htm`>, und mehr Informationen zur Administration der Module finden Sie unter „*System Management Guide: Operating System and Devices.*“ <`http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/aixbman/baseadmn/iandaadmin.htm`>

20.5.3.3 Das Konfigurieren von smb.conf

Einige Parameter werden in der Datei `smb.conf` benötigt, um das Verhalten von winbindd zu beeinflussen. Diese werden in der winbindd(8)-Manpage detaillierter beschrieben. Meine `smb.conf`, die in Beispiel **??** gezeigt wird, wurde verändert, um die notwendigen Einträge in den Abschnitt [global] einzubinden.

20.5.3.4 Den Samba-Server der Domäne des PDCs anschließen

Geben Sie den folgenden Befehl ein, um den Samba-Server der Domäne des PDCs anzuschließen, wobei *`DOMÄNE`* der Name Ihrer Windows-Domäne ist und *`Administrator`* der Name eines Domänen-Benutzers mit administrativen Rechten in der Domäne.

```
root#/usr/local/samba/bin/net rpc join -S PDC -U Administrator
```

Die richtige Antwort auf diesen Befehl sollte „*Joined the domain `DOMÄNE`*“ sein.

20.5.3.5 Starten und Testen des winbindd-Daemons

Sie wollen eventuell Ihr Samba-Startskript verändern, um den winbindd-Daemon automatisch aufzurufen, wenn die anderen Teile von Samba starten, aber es ist möglich, zuerst nur

Beispiel 20.5.1. smb.conf für Winbind

```
[global]
# Trenne Domäne und Benutzername durch '+', wie DOMÄNE+benutzername
        winbind separator = +
# Verwende UIDs von 10000 bis 20000 für Domänen-Benutzer
        idmap uid = 10000-20000
# Verwende GIDs von 10000 bis 20000 für Domänen-Gruppen
        idmap gid = 10000-20000
# Erlaube die Aufzählung von winbind-Benutzern und -Gruppen
        winbind enum users = yes
        winbind enum groups = yes
# Gib winbind-Benutzern eine echte Shell (nur benötigt, wenn diese telnet-Zugriff haben)
        template homedir = /home/winnt/%D/%U
        template shell = /bin/bash
```

den Winbind-Teil alleine zu testen. Um den Winbind-Dienst zu starten, geben Sie folgenden Befehl als root ein:

```
root#/usr/local/samba/bin/winbindd
```

ANMERKUNG

Obiges geht davon aus, dass Samba im Verzeichnis `/usr/local/samba` installiert wurde. Sie müssen nach dem Pfad Ihrer Samba-Dateien suchen, falls dies auf Ihrem System nicht der Pfad zu **winbindd** ist.

Winbindd kann mittlerweile auch im „*dual daemon mode*“ laufen. Das lässt ihn in Form von zwei Prozessen laufen. Der erste beantwortet alle Anfragen aus dem Cache und beschleunigt damit die Antworten an die Clients. Der andere Prozess aktualisiert den Cache für die Anfrage, die der erste Prozess gerade beantwortet hat. Der Vorteil all dessen ist, dass die Antworten schneller sind und trotzdem richtig bleiben. Sie aktivieren diesen Modus mit der Option `-B` auf der Befehlszeile:

```
root#/usr/local/samba/bin/winbindd -B
```

Ich bin immer paranoid und prüfe, dass der Daemon wirklich läuft:

```
root#ps -ae | grep winbindd
```

Dieser Befehl sollte eine Ausgabe wie die folgende erzeugen. Wenn der Daemon läuft, sollten Sie etwas wie das hier sehen:

```
3025 ?        00:00:00 winbindd
```

Nun zum Test in der Praxis, versuchen Sie, Informationen über die Benutzer auf Ihrem PDC zu erhalten:

```
root#/usr/local/samba/bin/wbinfo -u
```

Dies sollte eine Liste Ihrer Windows-Benutzer auf Ihrem PDC zurückgeben. Ich bekomme zum Beispiel das:

```
   CEO+Administrator
   CEO+burdell
   CEO+Guest
   CEO+jt-ad
   CEO+krbtgt
   CEO+TsInternetUser
```

Offensichtlich habe ich meine Domäne „*CEO*“ benannt, und mein winbind separator ist „+“.

Sie können dasselbe tun, um Gruppeninformationen vom PDC zu erhalten:

```
root# /usr/local/samba/bin/wbinfo -g
   CEO+Domain Admins
   CEO+Domain Users
   CEO+Domain Guests
   CEO+Domain Computers
   CEO+Domain Controllers
   CEO+Cert Publishers
   CEO+Schema Admins
   CEO+Enterprise Admins
   CEO+Group Policy Creator Owners
```

Die Funktion **getent** kann jetzt dafür verwendet werden, Gesamt-Listen sowohl von lokalen als auch von PDC-Benutzern und -Gruppen zu erhalten. Probieren Sie folgenden Befehl aus:

```
root#getent passwd
```

Sie sollten eine Liste erhalten, die wie Ihre Datei `/etc/passwd` aussieht, gefolgt von den Domänen-Benutzern mit ihren neuen UIDs, GIDs, home-Verzeichnissen und Standard-Shells.

Dasselbe kann für Gruppen geschehen:

```
root#getent group
```

20.5.3.6 Die init.d-Startskripten anpassen

Linux Der winbindd-Daemon muss starten, nachdem die smbd- und nmbd-Daemons laufen. Um diese Forderung zu erfüllen, müssen Sie die Start-Skripten Ihres Systems anpassen. Sie

finden sie in Red Hat Linux unter `/etc/init.d/smb` und in Debian Linux unter `/etc/init.d/samba`. Editieren Sie Ihr Skript, um den winbindd-Daemon in der richtigen Sequenz zu starten. Mein Start-Skript startet smbd, nmbd und winbindd direkt aus dem Verzeichnis `/usr/local/samba/bin`. Die Funktion **start** in diesem Skript sieht so aus:

```
start() {
        KIND="SMB"
        echo -n $"Start des Diensts $KIND: "
        daemon /usr/local/samba/bin/smbd $SMBDOPTIONS
        RETVAL=$?
        echo
        KIND="NMB"
        echo -n $"Start des Diensts $KIND: "
        daemon /usr/local/samba/bin/nmbd $NMBDOPTIONS
        RETVAL2=$?
        echo
        KIND="Winbind"
        echo -n $"Start des Diensts $KIND: "
        daemon /usr/local/samba/bin/winbindd
        RETVAL3=$?
        echo
        [ $RETVAL -eq 0 -a $RETVAL2 -eq 0 -a $RETVAL3 -eq 0 ] && \
      touch /var/lock/subsys/smb || RETVAL=1
        return $RETVAL
}
```

Wenn Sie winbindd im „*dual daemon mode*“ ausführen wollen, ersetzen Sie die Zeile

```
        daemon /usr/local/samba/bin/winbindd
```

in obigem Beispiel durch:

```
        daemon /usr/local/samba/bin/winbindd -B
```

.

Die Funktion **stop** hat einen korrespondierenden Eintrag, um die Dienste herunterzufahren, und sieht so aus:

```
stop() {
        KIND="SMB"
        echo -n $"Stoppen des Diensts $KIND: "
        killproc smbd
        RETVAL=$?
        echo
```

```
        KIND="NMB"
        echo -n $"Stoppen des Diensts $KIND: "
        killproc nmbd
        RETVAL2=$?
        echo
        KIND="Winbind"
        echo -n $"Stoppen des Diensts $KIND: "
        killproc winbindd
        RETVAL3=$?
        [ $RETVAL -eq 0 -a $RETVAL2 -eq 0 -a $RETVAL3 -eq 0 ] && \
       rm -f /var/lock/subsys/smb
        echo ""
        return $RETVAL
}
```

Solaris Winbind funktioniert nicht unter Solaris 9, lesen Sie dazu Abschnitt **??**.

Unter Solaris müssen Sie das Start-Skript `/etc/init.d/samba.server` editieren. Es startet üblicherweise nur smbd und nmbd, sollte jetzt aber auch winbindd starten. Wenn Sie Samba in `/usr/local/samba/bin` installiert haben, sollte die Datei etwas wie das hier enthalten:

```
##
## samba.server
##

if [ ! -d /usr/bin ]
then                    # /usr nicht gemountet
   exit
fi

killproc() {            # kill den/die angegebenen Prozess(e)
   pid=‘/usr/bin/ps -e |
        /usr/bin/grep -w $1 |
        /usr/bin/sed -e ’s/^  *//’ -e ’s/ .*//’‘
   [ "$pid" != "" ] && kill $pid
}

# Starte/stoppe die für den Samba-Server erforderlichen Prozesse


case "$1" in

’start’)
#
# Editieren Sie diese Zeilen passend zu Ihrer Installation
# (Pfade, Arbeitsgruppe, Host)
#
```

```
echo Starten von SMBD
   /usr/local/samba/bin/smbd -D -s \
   /usr/local/samba/smb.conf

echo Starten von NMBD
   /usr/local/samba/bin/nmbd -D -l \
   /usr/local/samba/var/log -s /usr/local/samba/smb.conf

echo Starten von WINBINDD
   /usr/local/samba/bin/winbindd
   ;;

'stop')
   killproc nmbd
   killproc smbd
   killproc winbindd
   ;;

*)
   echo "Usage: /etc/init.d/samba.server { start | stop }"
   ;;
esac
```

Auch hier gilt: Wenn Sie Samba im „*dual daemon mode*“ ausführen wollen, ersetzen Sie

```
/usr/local/samba/bin/winbindd
```

in obigem Skript durch:

```
/usr/local/samba/bin/winbindd -B
```

Neustart Wenn Sie an diesem Punkt die Daemons smbd, nmbd und winbindd neu starten, sollten Sie sich als Domänen-Mitglied genauso mit dem Samba-Server verbinden können, als ob Sie ein lokaler Benutzer wären.

20.5.3.7 Winbind und PAM konfigurieren

Wenn Sie es bis hierher geschafft haben, wissen Sie, dass **winbindd** und Samba zusammenarbeiten. Wenn Sie Winbind dazu verwenden wollen, Authentifikation für andere Dienste anzubieten, lesen Sie weiter. Die PAM-Konfigurationsdateien müssen in diesem Schritt verändert werden. (Haben Sie auch nicht vergessen, Backups der Dateien in `/etc/pam.d` anzulegen? Wenn doch, sichern Sie sie jetzt.)

Sie brauchen ein PAM-Modul, um winbindd mit diesen anderen Diensten zu verwenden. Dieses Modul wird im Verzeichnis `../source/nsswitch` kompiliert, indem Sie den Befehl

```
root#make nsswitch/pam_winbind.so
```

im Verzeichnis `../source` ausführen. Die Datei `pam_winbind.so` sollte zu Ihren anderen PAM-Sicherheitsmodulen kopiert werden. Auf meinem RedHat-System war das das Verzeichnis `/lib/security`. Unter Solaris liegen die PAM-Sicherheitsmodule in `/usr/lib/security`:

```
root#cp ../samba/source/nsswitch/pam_winbind.so /lib/security
```

Linux/FreeBSD-spezifische PAM-Konfiguration Die Datei `/etc/pam.d/samba` muss nicht verändert werden. Ich habe diese Datei einfach so belassen, wie sie war:

```
auth    required        /lib/security/pam_stack.so service=system-auth
account required        /lib/security/pam_stack.so service=system-auth
```

Die anderen Dienste, die ich modifiziert habe, um die Verwendung von Winbind als Authentifikationsdienst zu erlauben, waren der normale Konsolen-Login (oder eine Terminal-Session), telnet-logins und der ftp-Dienst. Um diese Dienste zu aktivieren, müssen Sie zuerst die Einträge in `/etc/xinetd.d` (oder `/etc/inetd.conf`) ändern. Red Hat Linux ab Version 7.1 verwendet die neue xinetd.d-Struktur. In diesem Fall müssen Sie die Zeilen in `/etc/xinetd.d/telnet` und `/etc/xinetd.d/wu-ftp` ändern.

```
enable = no
```

wird zu:

```
enable = yes
```

Damit der ftp-Dienst ordnungsgemäß arbeitet, müssen Sie auch die einzelnen Verzeichnisse für die Domänen-Benutzer auf dem Server angelegt haben oder das home-Verzeichnis für die Domänen-Benutzer auf ein allgemeines, gemeinsames Verzeichnis für alle Domänen-Benutzer gesetzt haben. Das kann einfach dadurch geschehen, dass Sie den globalen Eintrag template homedir in `smb.conf` setzen.

Die Datei `/etc/pam.d/ftp` kann verändert werden, um den ftp-Zugriff in derselben Art wie den Samba-Zugriff zu erlauben. Meine Datei `/etc/pam.d/ftp` wurde so verändert:

```
auth       required     /lib/security/pam_listfile.so item=user sense=deny \
    file=/etc/ftpusers onerr=succeed
auth       sufficient   /lib/security/pam_winbind.so
auth       required     /lib/security/pam_stack.so service=system-auth
auth       required     /lib/security/pam_shells.so
account    sufficient   /lib/security/pam_winbind.so
account    required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
```

Die Datei `/etc/pam.d/login` kann fast genauso verändert werden. Sie sieht jetzt so aus:

```
auth       required     /lib/security/pam_securetty.so
auth       sufficient   /lib/security/pam_winbind.so
auth       sufficient   /lib/security/pam_UNIX.so use_first_pass
auth       required     /lib/security/pam_stack.so service=system-auth
auth       required     /lib/security/pam_nologin.so
account    sufficient   /lib/security/pam_winbind.so
account    required     /lib/security/pam_stack.so service=system-auth
password   required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
session    optional     /lib/security/pam_console.so
```

In diesem Fall habe ich die Zeilen

```
auth sufficient /lib/security/pam_winbind.so
```

wie zuvor hinzugefügt, aber auch davor

```
required pam_securetty.so
```

eingefügt, um root-Logins über das Netzwerk zu verbieten. Ich habe auch eine Zeile

```
sufficient /lib/security/pam_unix.so use_first_pass
```

nach der **winbind.so**-Zeile eingefügt, um die nervenden Doppel-Aufforderungen nach dem Passwort loszuwerden.

Solaris-spezifische Konfiguration Die Datei `/etc/pam.conf` muss geändert werden. Ich habe diese Datei so geändert, dass meine Domänen-Benutzer sich sowohl lokal als auch über telnet anmelden können. Sie können die Datei `pam.conf` an Ihre Bedürfnisse anpassen, aber sorgen Sie dafür, dass Sie wissen, was Sie tun, da diese Änderungen im schlimmsten Fall Ihre Maschine in einem nahezu nicht-startfähigen Zustand zurücklassen. Ich habe Folgendes geändert:

```
#
#ident "@(#)pam.conf 1.14 99/09/16 SMI"
#
# Copyright (c) 1996-1999, Sun Microsystems, Inc.
# All Rights Reserved.
#
# PAM configuration
#
# Authentication management
#
login   auth required   /usr/lib/security/pam_winbind.so
login auth required  /usr/lib/security/$ISA/pam_UNIX.so.1 try_first_pass
login auth required  /usr/lib/security/$ISA/pam_dial_auth.so.1 try_first_pass
#
```

```
rlogin  auth sufficient /usr/lib/security/pam_winbind.so
rlogin  auth sufficient /usr/lib/security/$ISA/pam_rhosts_auth.so.1
rlogin auth required  /usr/lib/security/$ISA/pam_UNIX.so.1 try_first_pass
#
dtlogin auth sufficient /usr/lib/security/pam_winbind.so
dtlogin auth required  /usr/lib/security/$ISA/pam_UNIX.so.1 try_first_pass
#
rsh auth required /usr/lib/security/$ISA/pam_rhosts_auth.so.1
other   auth sufficient /usr/lib/security/pam_winbind.so
other auth required /usr/lib/security/$ISA/pam_UNIX.so.1 try_first_pass
#
# Account management
#
login   account sufficient      /usr/lib/security/pam_winbind.so
login account requisite /usr/lib/security/$ISA/pam_roles.so.1
login account required /usr/lib/security/$ISA/pam_UNIX.so.1
#
dtlogin account sufficient      /usr/lib/security/pam_winbind.so
dtlogin account requisite /usr/lib/security/$ISA/pam_roles.so.1
dtlogin account required /usr/lib/security/$ISA/pam_UNIX.so.1
#
other   account sufficient      /usr/lib/security/pam_winbind.so
other account requisite /usr/lib/security/$ISA/pam_roles.so.1
other account required /usr/lib/security/$ISA/pam_UNIX.so.1
#
# Session management
#
other session required /usr/lib/security/$ISA/pam_UNIX.so.1
#
# Password management
#
#other   password sufficient     /usr/lib/security/pam_winbind.so
other password required /usr/lib/security/$ISA/pam_UNIX.so.1
dtsession auth required /usr/lib/security/$ISA/pam_UNIX.so.1
#
# Support for Kerberos V5 authentication (uncomment to use Kerberos)
#
#rlogin auth optional /usr/lib/security/$ISA/pam_krb5.so.1 try_first_pass
#login auth optional /usr/lib/security/$ISA/pam_krb5.so.1 try_first_pass
#dtlogin auth optional /usr/lib/security/$ISA/pam_krb5.so.1 try_first_pass
#other auth optional /usr/lib/security/$ISA/pam_krb5.so.1 try_first_pass
#dtlogin account optional /usr/lib/security/$ISA/pam_krb5.so.1
#other account optional /usr/lib/security/$ISA/pam_krb5.so.1
#other session optional /usr/lib/security/$ISA/pam_krb5.so.1
#other password optional /usr/lib/security/$ISA/pam_krb5.so.1 try_first_pass
```

Ich habe auch hier eine Zeile *try_first_pass* nach der Zeile mit `winbind.so` eingefügt, um die Doppel-Aufforderungen nach den Passwörtern loszuwerden.

Jetzt starten Sie Samba neu und versuchen, sich über die jeweilige Anwendung zu verbinden, die Sie in pam.conf konfiguriert haben.

20.6 Zusammenfassung

Das Winbind-System erlaubt unter Verwendung des Name Service Switch, der Pluggable-Authentication-Module und entsprechender Microsoft RPC-Aufrufe die nahtlose Integration von Microsoft Windows NT-Domänen-Benutzern in ein UNIX-System. Das Ergebnis ist eine große Verringerung des administrativen Aufwands, der zum Betrieb eines gemischten UNIX- und NT-Netzwerks erforderlich ist.

20.7 Gängige Fehler

Winbind hat eine Anzahl von Einschränkungen in der derzeit veröffentlichten Version. Wir hoffen, diese in zukünftigen Versionen beseitigen zu können:

- Winbind ist derzeit nur für die Betriebssysteme Linux, Solaris, AIX und IRIX verfügbar, obwohl Portierungen auf andere Betriebssysteme sicherlich möglich sind. Um solche Portierungen zu ermöglichen, ist es erforderlich, dass die C-Library des jeweiligen Betriebssystems die Systeme Name Service Switch (NSS) und Pluggable Authentication Modules (PAM) unterstützt. Das wird immer gängiger, da NSS und PAM immer mehr Unterstützung von UNIX-Herstellern gewinnen.
- Die Zuordnungen von Windows NT-RIDs zu UNIX-IDs wird nicht algorithmisch durchgeführt und hängt von der Reihenfolge ab, in der die nicht-zugeordneten Benutzer/Gruppen von Winbind gesehen werden. Es kann schwierig werden, die RID-zu-UNIX-ID-Zuordnungen wiederherzustellen, wenn die Datei, die diese Information enthält, beschädigt oder zerstört ist.
- Derzeit berücksichtigt das Winbind-PAM-Modul die möglichen Zeitbeschränkungen nicht, die für Windows NT-Domänen-Benutzer gesetzt sein können (Workstation- und Login-Zeitbeschränkungen); diese muss der PDC erzwingen.

20.7.1 Warnung vor Problemen durch NSCD

> **Warnung**
>
> Führen Sie unter keinen Umständen **nscd** auf irgendeinem System aus, auf dem **winbindd** läuft.

Wenn **nscd** auf dem UNIX/Linux-System läuft, wird es selbst dann, wenn NSSWITCH korrekt konfiguriert ist, nicht möglich sein, die Namen von Domänen-Benutzern und -Gruppen aufzulösen.

20.7.2 Winbind löst keine Benutzer- und Gruppen-Namen auf

„*Meine Datei* `smb.conf` *ist ordnungsgemäß konfiguriert. Ich habe idmap uid = 12000 und idmap gid = 3000-3500 angegeben, und* ***winbind*** *läuft. Wenn ich Folgendes tue, funktioniert es prächtig:*“

```
root# wbinfo -u
MITTELERDE+maryo
MITTELERDE+jackb
MITTELERDE+ameds
...
MITTELERDE+root

root# wbinfo -g
MITTELERDE+Domain Users
MITTELERDE+Domain Admins
MITTELERDE+Domain Guests
...
MITTELERDE+Accounts

root# getent passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
...
maryo:x:15000:15003:Mary Orville:/home/MITTELERDE/maryo:/bin/false
```

„*Aber dieser Befehl schlägt fehl:*

```
root# chown maryo a_file
chown: 'maryo': invalid user
```

Das macht mich verrückt! Was kann da falsch sein?“

Das ist dasselbe Problem wie oben. Ihr System führt höchstwahrscheinlich **nscd** aus. Stoppen Sie diesen Dienst, und starten Sie ihn nicht mehr! Ihr Problem wird gelöst sein.

Kapitel 21

FORTGESCHRITTENES NETZWERK-MANAGEMENT

Dieser Abschnitt dokumentiert Randthemen, die sehr wichtig für Netzwerkadministratoren sind, die die Zugriffskontrolle auf Netzwerk-Ressourcen verbessern, die Benutzerumgebung automatisieren und ihr Leben ein wenig erleichtern möchten.

21.1 Eigenschaften und Vorzüge

Oft kann der Unterschied zwischen einer funktionierenden Netzwerkumgebung und einer als gut wahr- und angenommenen Netzwerkumgebung am besten durch die *Kleinigkeiten* gemessen werden, die alles noch harmonischer arbeiten lassen. Eine Schlüsselrolle bei jeder Netzwerklösung ist die Fähigkeit, per Fernzugriff MS Windows-Workstations warten zu können, über das Netz auf den Samba-Server zugreifen zu können, angepasste Anmelde-Skripten zur Verfügung stellen zu können und andere „*Hausarbeiten*“ erledigen zu können, die helfen, einen verlässlicheren Netzwerk-Betrieb zu erreichen.

Dieses Kapitel präsentiert Informationen zu jedem dieser Bereiche. Sie wurden hier und nicht in anderen Kapiteln platziert, um das Nachschlagen zu erleichtern.

21.2 Server-Fernwartung

„*Wie bekomme ich einen 'User Manager' und 'Server Manager'?*“

Da ich ja keinen NT4 Server kaufen muss, wie bekomme ich den 'User Manager for Domains' und den 'Server Manager'?

Microsoft vertreibt eine Version dieser Tools namens `Nexus.exe` zur Installation auf Windows 9x/Me-Systemen. Dieses Set enthält:

- Server Manager
- User Manager for Domains
- Event Viewer

Laden Sie die Archivdatei von <ftp://ftp.microsoft.com/Softlib/MSLFILES/NEXUS.EXE> herunter.

Die Windows NT 4.0-Version des 'User Manager for Domains' und 'Server Manager' sind über ftp bei Microsoft erhältlich <ftp://ftp.microsoft.com/Softlib/MSLFILES/SRVTOOLS.EXE>.

21.3 Desktop-Fernwartung

Es gibt eine Reihe von verfügbaren Desktop-Fernwartungslösungen, die von gratis bis teuer reichen. Lassen Sie sich davon nicht abhalten. Manchmal ist die teuerste Lösung die kosteneffektivste. In jedem Fall müssen Sie Ihre eigenen Schlüsse ziehen, was die beste Lösung für Ihr Netzwerk ist.

21.3.1 Fernwartung von NoMachine.Com

Folgende Informationen wurden auf der Samba-Mailingliste am 3.4.2003 um 23:33:50 GMT gepostet. Sie werden in abgewandelter Form präsentiert (mit fehlenden Autorenangaben wegen des Datenschutzes). Die gesamte Antwort wird (bis auf ein paar Kommentare) gezeigt.

„*Ich habe einen wunderbaren Linux/Samba-Server als PDC laufen. Jetzt würde ich gerne Fernwartungsfunktionen hinzufügen, so dass Benutzer sich am System anmelden und ihren Desktop von Zuhause aus oder aus dem Ausland erreichen können.*"

„*Gibt es eine Möglichkeit, dies zu erreichen? Brauche ich einen Windows Terminal Server? Muss ich ihn so konfigurieren, dass er Domänen-Mitglied ist oder ein BDC, PDC? Gibt es irgendwelche Hacks für Windows XP, um Fernzugriff zu aktivieren, auch wenn der Rechner in einer Domäne ist?*"

Gegebene Antwort: Prüfen Sie das neue Angebot der „*NX*"-Software von NoMachine <http://www.nomachine.com/>.

Es implementiert ein leicht zu verwendendes Interface zum Remote-X-Protokoll und schließt VNC/RFB und rdesktop/RDP ein, dies jedoch mit einer Geschwindigkeit, wie Sie sie wahrscheinlich noch nicht gesehen haben.

Remote X ist bei weitem nicht neu, aber was hier erreicht wurde, ist eine neue Art von Kompressions- und Caching-Technologie, die diese Software sogar über langsame Modem/ISDN-Strecken ausreichend schnell laufen lässt.

Ich konnte die (öffentliche) RedHat-Maschine von NoMachine in Italien über eine belastete Internet-Verbindung mit aktivierten Thumbnails im KDE Konqueror „*testfahren*", der unverzüglich auf „*mouse-over*" ansprang. Aus dieser (remote X) Sitzung heraus startete ich eine rdesktop-Sitzung auf eine weitere Windows XP-Maschine. Um die Performance zu testen, spielte ich Pinball. Ich bin stolz, sagen zu dürfen, dass ich beim ersten Versuch 631750 Punkte erreichte.

NX arbeitet in meinem LAN besser als die anderen „*reinen*" Verbindungsarten, die ich von Zeit zu Zeit benutze: TightVNC, rdesktop oder Remote X. Es ist sogar schneller als eine direkte Crosslink-Verbindung zwischen zwei Knoten.

Ich bekomme sogar Sound von der Remote-X-Applikation auf meine lokalen Lautsprecher, und ich hatte ein funktionierendes „*copy'n'paste*“ von einem NX-Fenster (in dem eine KDE-Sitzung in Italien lief) in meinen Mozilla-Mail-Agenten. Die Leute bei NoMachine machen definitiv etwas richtig!

Ich empfehle jedem, der auch nur ein nebensächliches Interesse an Fernwartung hat, NX auszuprobieren: <`http://www.nomachine.com/testdrive.php`>.

Laden Sie einfach den kostenlosen Client herunter (verfügbar für Red Hat, SuSE, Debian und Windows), und innerhalb von fünf Minuten geht es los (es müssen allerdings erst die Zugangsdaten gesendet werden, weil Sie einen vollen UNIX-Account auf deren testdrive.nomachine.com-Maschine erhalten).

NoMachine plant eine Ausbaustufe, auf der Sie einen NX-Applikationsserver als Cluster betreiben können. Die Benutzer starten einfach eine lokale NX-Session und können Applikationen auswählen, die transparent laufen (Anwendungen können sogar auf einem anderen NX-Knoten laufen, aber vorgeben, auf demselben Knoten zu sein wie der, an dem sich der Benutzer angemeldet hat, weil er im selben Fenster angezeigt wird. Sie können sie auch fullscreen ausführen, und nach kurzer Zeit vergessen Sie überhaupt, dass es eine Remote-Session ist).

Nun das Beste am Schluss: All die Kerntechnologien zur Kompression und zum Caching werden unter der GPL veröffentlicht und sind als Sourcecode für jeden verfügbar, der darauf aufbauen will! Diese Technologien funktionieren, wenn auch nur von der Befehlszeile aus (und sind sehr unpraktisch zu gebrauchen, um eine voll funktionsfähige Remote-X-Session zum Laufen zu bringen.)

Um Ihre Fragen zu beantworten:

- Sie müssen keinen Terminal-Server installieren; in XP ist eine RDP-Unterstüzung integriert.
- NX ist viel billiger als Citrix — und vergleichbar in der Performance, wenn nicht schneller.
- Sie müssen XP nicht hacken, es funktioniert einfach.
- Sie melden sich an der XP-Box transparent aus der Ferne an (und ich glaube, es gibt keinen Anlass, etwas zu ändern, um eine Verbindung zu bekommen, sogar, wenn die Authentifikation an einer Domäne erfolgt).
- Die NX-Kern-Technologien sind alle OpenSource und unter der GPL — veröffentlicht. Sie können jetzt eine (sehr unbequeme) Befehlszeile kostenlos nutzen, oder Sie können ein komfortables (proprietäres) NX-GUI-Frontend kaufen.
- NoMachine ermutigt und unterstützt OSS/Free-Software-Implementierungen auch für ein solches Frontend, sogar wenn es für sie Konkurrenz bedeutet (sie haben dies sogar in den Entwickler-Listen für LTSP, KDE und GNOME geschrieben).

21.4 Die „*Magie*“ von Netzwerk-Anmeldeskripten

Es gibt mehrere Möglichkeiten, um eine angepasste Konfiguration der Netzwerk-Start-Umgebung zu schaffen.

- Kein Anmeldeskript
- Ein simples und universelles Anmeldeskript, das für alle Benutzer verwendet wird
- Verwendung eines von Bedingungen abhängigen Skripts, das je nach Benutzer- oder Gruppen-Attributen angewendet wird
- Anwendung von Sambas preexec- und postexec-Funktionen beim Zugriff auf die NETLOGON-Freigabe, um ein angepasstes Anmeldeskript zu generieren und auszuführen
- Verwendung eines Tools wie KixStart

Der Quelltext-Tree von Samba enthält zwei Werkzeuge zum Generieren und Ausführen von Anmeldeskripten (siehe die Sub-Verzeichnisse `genlogon` und `ntlogon` im Verzeichnis `examples`).

Die folgenden Listings stammen aus dem Verzeichnis `genlogon`.

Dies ist die Datei `genlogon.pl`:

```
#!/usr/bin/perl
#
# genlogon.pl
#
# Perl script to generate user logon scripts on the fly, when users
# connect from a Windows client. This script should be called from
# smb.conf with the %U, %G and %L parameters. I.e:
#
#       root preexec = genlogon.pl %U %G %L
#
# The script generated will perform
# the following:
#
# 1. Log the user connection to /var/log/samba/netlogon.log
# 2. Set the PC's time to the Linux server time (which is maintained
#    daily to the National Institute of Standards Atomic clock on the
#    internet.
# 3. Connect the user's home drive to H: (H for Home).
# 4. Connect common drives that everyone uses.
# 5. Connect group-specific drives for certain user groups.
# 6. Connect user-specific drives for certain users.
# 7. Connect network printers.

# Log client connection
#($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst) = localtime(time);
($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst) = localtime(time);
open LOG, ">>/var/log/samba/netlogon.log";
print LOG "$mon/$mday/$year $hour:$min:$sec";
print LOG " - User $ARGV[0] logged into $ARGV[1]\n";
close LOG;
```

```
# Start generating logon script
open LOGON, ">/shared/netlogon/$ARGV[0].bat";
print LOGON "\@ECHO OFF\r\n";

# Connect shares just use by Software Development group
if ($ARGV[1] eq "SOFTDEV" || $ARGV[0] eq "softdev")
{
   print LOGON "NET USE M: \\\\$ARGV[2]\\SOURCE\r\n";
}

# Connect shares just use by Technical Support staff
if ($ARGV[1] eq "SUPPORT" || $ARGV[0] eq "support")
{
   print LOGON "NET USE S: \\\\$ARGV[2]\\SUPPORT\r\n";
}

# Connect shares just used by Administration staff
If ($ARGV[1] eq "ADMIN" || $ARGV[0] eq "admin")
{
   print LOGON "NET USE L: \\\\$ARGV[2]\\ADMIN\r\n";
   print LOGON "NET USE K: \\\\$ARGV[2]\\MKTING\r\n";
}

# Now connect Printers. We handle just two or three users a little
# differently, because they are the exceptions that have desktop
# printers on LPT1: - all other user's go to the LaserJet on the
# server.
if ($ARGV[0] eq 'jim'
    || $ARGV[0] eq 'yvonne')
{
   print LOGON "NET USE LPT2: \\\\$ARGV[2]\\LJET3\r\n";
   print LOGON "NET USE LPT3: \\\\$ARGV[2]\\FAXQ\r\n";
}
else
{
   print LOGON "NET USE LPT1: \\\\$ARGV[2]\\LJET3\r\n";
   print LOGON "NET USE LPT3: \\\\$ARGV[2]\\FAXQ\r\n";
}

# All done! Close the output file.
close LOGON;
```

Diejenigen, die sich ein weiter ausgeführtes oder mächtigeres Anmeldesystem wünschen, mögen folgende Seiten aufsuchen:

- <http://www.craigelachie.org/rhacer/ntlogon>

- <http://www.kixtart.org>

21.4.1 Hinzufügen von Druckern ohne Benutzer-Eingriff

Drucker können automatisch während des Anmeldevorgangs hinzugefügt werden, wenn Sie

```
C:\> rundll32 printui.dll,PrintUIEntry /?
```

benutzen (siehe die Dokumentation in Microsoft Knowledgebase Artikel 189105. <http://support.microsoft.com/default.asp?scid=kb;en-us;189105>)

Kapitel 22

SYSTEM UND ZUGRIFFSRICHTLINIEN

Dieses Kapitel fasst den gegenwärtigen Wissensstand aus praktischer Arbeit und Erkenntnissen in der Samba-Mailingliste zusammen. Vor einer reinen Wiedergabe dieser veröffentlichten Informationen wurde jede Anstrengung unternommen, diese gewonnenen Informationen zu prüfen. Wo zusätzliche Informationen durch diese Prüfungen entdeckt wurden, werden diese ebenfalls zur Verfügung gestellt.

22.1 Eigenschaften und Vorzüge

Als MS Windows NT 3.5 vorgestellt wurde, war das neue heiße Thema die Fähigkeit, Gruppenrichtlinien für Benutzer und Gruppen zu implementieren. Dann kam MS Windows NT 4, und einige Sites begannen damit, diese Möglichkeiten zu übernehmen. Woher wir das wissen? Durch die Anzahl von „*boo-boos*“ (oder Fehlern), die Administratoren machten, und durch deren anschließende Bitten um Hilfe bei der Lösung.

Zu der Zeit, als MS Windows 2000 und Active Directory veröffentlicht wurden, bekamen die Administratoren das Signal: Gruppen-Richtlinien sind etwas Gutes! Sie helfen, Administrationskosten zu senken und machen Benutzer einfach glücklicher. Aber das wahre Potenzial der MS Windows 200x Active Directory- und Gruppen-Richtlinien-Objekte (GPOs) für Benutzer und Maschinen wurde nur zögerlich angenommen. Dies konnte man daran erkennen, dass auf der Samba-Mailingliste in den Jahren 2000 und 2001 nur wenige Anfragen zu den GPOs und deren Nutzung in einer Samba-Umgebung gestellt wurden.

Wenn wir von dem Traffic-Volumen seit Mitte des Jahres 2002 ausgehen, wurden GPOs ein grundlegender Bestandteil von Entwicklungen vielerorts. Dieses Kapitel betrachtet Techniken und Methoden, die dazu genutzt werden können, Vorteile bei der Automatisierung der Kontrolle über Benutzeroberflächen und vernetzte Client-Arbeitsplätze zu erzielen.

In diesem Dokunent wird ebenfalls ein neues Samba-Werkzeug beschrieben — das **editreg** Werkzeug — , das in Zukunft ein wichtiger Bestandteil der Arbeit von Samba-Administratoren werden könnte.

22.2 Anlegen und Verwalten von System-Richtlinien

Auf MS Windows-Plattformen, speziell auf denen, die den Veröffentlichungen von MS Windows NT4 und MS Windows 95 folgten, ist es möglich, einen Dateityp zu erzeugen, der in der NETLOGON-Freigabe des Domänencontrollers abgelegt werden kann. Sobald sich ein Client am Netzwerk anmeldet, wird diese Datei ausgelesen und der Inhalt dazu benutzt, Änderungen an der Registry der Clientmaschine durchzuführen. Diese Datei erlaubt Änderungen an den Teilen der Registry, die die Benutzer, Benutzergruppen oder Maschinen betreffen.

Für MS Windows 9x/ME muss diese Datei `Config.POL` heißen. Sie kann dadurch erzeugt werden, daß das Werkzeug `poledit.exe`, auch besser unter dem Namen „*Policy Editor*“ bekannt, benutzt wird. Der „*Policy Editor*“ wurde auf der Windows 98-Installations-CD zur Verfügung gestellt, aber verschwand wieder durch die Einführung von MS Windows Me (Millenium Edition). Nach Angaben von MS Windows-Netzwerk-Administratoren sollte dieses Werkzeug Bestandteil des MS Windws Me Resource Kits werden.

MS Windows NT4 Server-Produkte enthalten den *System-Richtlinien-Editor* unterhalb von **Start** -> **Programme** -> **Administrations-Werkzeuge**. Für MS Windows NT4 und spätere Clients muss diese Datei `NTConfig.POL` heißen.

Die Microsoft Management Konsole (MMC) war eine Neuheit von MS Windows 2000. Dieses Werkzeug ist die neue Welle in der sich ständig ändernden Landschaft der Methoden, die Microsoft für das Management von Netzwerk-Zugriff und -Sicherheit einsetzt. Jedes neue Microsoft-Produkt oder jede neue Technologie scheint die alten Regeln überflüssig zu machen und führt gleichzeitig neuere und wieder komplexere Werkzeuge und Methoden ein. Zu Microsofts Ehrenrettung muss man sagen, dass MMC ein Schritt vorwärts war, aber die gesteigerte Funktionalität hat auch einen großen Preis.

Bevor wir die Konfiguration von Netzwerk- und System-Richtlinien in Angriff nehmen, ist es höchst ratsam, die unter Implementing Profiles and Policies in Windows NT 4.0 <`http://www.microsoft.com/ntserver/management/deployment/planguide/prof_policies.asp`> erhältliche Dokumentation von Microsofts Webseite zu beachten. Es gibt eine große Anzahl von zusätzlichen Dokumenten zu dieser etwas älteren Dokumentation, die Sie ebenso lesen und verstehen sollten. Versuchen Sie, auf der Microsoft-Webseite nach „*Gruppen Richtlinien*“ zu suchen.

Nachfolgend finden Sie eine kurze Erörterung des Themas mit einigen hilfreichen Anmerkungen. Diese Informationen sind nicht vollständig — Sie wurden gewarnt!

22.2.1 Windows 9x/ME-Richtlinien

Sie benötigen den Gruppen-Richtlinien-Editor von Windows 98, um Gruppenrichtlinien unter Windows 9x/Me zu bearbeiten. Diesen finden Sie auf der Original-CD einer Vollversion von Windows 98 unterhalb von `tools/reskit/netadmin/poledit`. Installieren Sie ihn, indem Sie „*Hinzufügen/Entfernen von Programmen*“ verwenden und dann auf **Datenträger** klicken.

Benutzen Sie den Gruppen-Richtlinien-Editor, um eine Richtliniendatei zu erzeugen, die den Ort der Benutzerrichtlinien und/oder `Eigene Dateien` festlegt und so weiter. Dann

speichern Sie diese Einstellungen in einer Datei namens `Config.POL`, die Sie im Hauptverzeichnis der Freigabe *`[NETLOGON]`* ablegen. Falls Sie Windows 98 zum Anmelden an der Samba-Domäne konfiguriert haben, so wird diese Datei automatisch gelesen und die Windows 9x/Me-Registry der Maschine beim Anmelden aktualisiert.

Weitere Details werden in der Dokumentation zum Windows 98 Resource Kit behandelt.

Falls Sie sich nicht an die korrekten Schritte halten, wird es oft dazu kommen, dass Windows 9x/Me die Integrität der Registry überprüft und anschließend seine Einstellungen aus der Sicherungskopie der Registry wiederherstellt, die sich auf jeder Windows 98/Me-Maschine befindet. Also werden Sie vielleicht bemerken, dass gelegentlich Einstellungen auf ihren Originalwert zurückgesetzt werden.

Installieren Sie den Systemrichtlinien-Editor von Windows 9x/Me, um Gruppenrichtlinien zu benutzen. Sehen Sie dazu auf der Windows 98-CD in `tools\reskit\netadmin\poledit` nach. Installieren Sie die Gruppenrichtlinien, indem Sie auf die Datei `grouppol.inf` doppelklicken. Melden Sie sich mehrmals ab und wieder an, und beobachten Sie, ob Windows 98 die Guppenrichtlinien annimmt. Leider müssen Sie dies für jede Windows 98/Me-Maschine machen, die Gruppenrichtlinien nutzen soll.

22.2.2 Windows NT4-Richtlinien-Dateien

Um die Datei `ntconfig.pol` zu erzeugen oder zu editieren, müssen Sie den NT Server-Richtlinieneditor **poledit.exe** benutzen, der nicht in NT Workstation, sondern nur in NT4 Server enthalten ist. Es gibt zwar einen Richtlinieneditor in NT Workstation, dieser eignet sich jedoch nicht, um Domänen-Richtlinien zu erzeugen. Ebenso könnte man den Richtlinien-Editor von Windows 95 auf NT4 Workstation/Server installieren; dieser arbeitet jedoch nicht mit NT-Clients. Die Dateien vom NT Server werden jedoch gut mit einer NT4-Workstation laufen.

Sie benötigen `poledit.exe`, `common.adm` und `winnt.adm`. Es ist zweckmäßig, die beiden `*.adm`-Dateien in das Verzeichnis `c:\winnt\inf` zu legen, das dazu dient, dass das Programm hier nachschaut (wenn nichts anderes eingestellt ist). Dieses Verzeichnis ist normalerweise „*Versteckt (Hidden)*.“

Der Richtlinien-Editor für Windows NT 4.0 ist ebenfalls im Service Pack 3 (und später) enthalten. Entpacken Sie die Datei durch **servicepackname /x**, dies wäre für Service Pack 6a **Nt4sp6ai.exe /x**. Der Richtlinien-Editor **poledit.exe** und die zugehörigen Vorlagendateien (*.adm) sollten ebenfalls ausgepackt werden. Es ist des Weiteren möglich, die Richtlinien-Vorlagen für Office 97 und somit eine Kopie des Richtlinien-Editors downzuloaden. Eine mögliche weitere Quelle stellt das Zero Administration Kit als Download von Microsoft dar.

22.2.2.1 Die Registry „*verderben*“

Mit NT4 änderten sich Registry-basierende Richtlinien: Eine große Anzahl von Einstellungen werden nicht automatisch zurückgesetzt, wenn der Benutzer sich abmeldet. Die Einstellungen, die in der Datei `NTConfig.POL` in die Arbeitsstations-Registry des Clients gesetzt werden und durch den Registrykey HKEY_LOCAL_MACHINE bereits gesetzt sind, bleiben so lange bestehen, bis sie anderweitig zurückgesetzt werden. Dies ist auch als „*tatooing*“

bekannt. Es kann ernsthafte Probleme damit geben, und der Administrator muss extrem vorsichtig im Umgang damit sein, um sich nicht die Möglichkeit zu verbauen, die Maschine später noch verwalten zu können.

22.2.3 MS Windows 200x/XP Professional-Richtlinien

Windows NT4-System-Richtlinien erlauben das Setzen von Registry-Parametern für Benutzer, Gruppen und Maschinen (Client-Workstations), die Mitglied einer NT4-Domäne sind. Derartige Richtlinien-Dateien werden mit Windows 200x/XP-Clients ebenfalls funktionieren.

Als Neuigkeit in Windows 2000 stellte Microsoft kürzlich eine Art von Gruppenrichtlinien vor, die, verglichen mit NT4-Richtlinien, eine Erweiterung der Möglichkeiten darstellten. Natürlich ist das Werkzeug zum Erzeugen wieder anders. und die Mechanismen für die Einbindung sind deutlich erweitert.

Die älteren NT4-basierenden Registry-Richtlinien sind als *Administrative Vorlagen* in MS Windows 2000/XP-Gruppen-Richtlinien-Objekten (GPOs) bekannt. Diese beinhalten die Möglichkeit, zahlreiche Sicherheitskonfigurationen zu setzen, Browser-Einstellungen des Internet Explorers zu erzwingen und Aspekte zu ändern und umzuleiten, die den Benutzer-Desktop betreffen (inklusive des Pfads zu `Eigene Dateien` (Verzeichnis) sowie der Möglichkeit zu beeinflussen, an welcher Stelle im Start-Menü Einträge erscheinen sollen). Ein weiteres neues Feature ist die Möglichkeit, bestimmte Windows-Software bestimmten Benutzern und/oder Gruppen zuzuordnen.

Denken Sie daran, dass NT4-Richtlinien-Dateien `NTConfig.POL` heißen und im Hauptverzeichnis der NETLOGON-Freigabe des Domänencontrollers gespeichert werden. Ein Windows NT4-Benutzer gibt einen Benutzernamen und ein Passwort ein und wählt dann den Namen der Domäne aus, an der er sich anmelden möchte. Während des Anmeldeprozesses liest die Client-Machine die Datei `NTConfig.POL` aus der NETLOGON-Freigabe aus und modifiziert die lokalen Registry- Einstellungen gemäß den Werten in dieser Datei.

Windows 200x-GPOs (Gruppenrichtlinien-Objekte) bieten viele Möglichkeiten. Sie werden nicht in der NETLOGON-Freigabe gespeichert, denn ein Teil einer Windows 200x-Richtlinie wird in Active Directory selbst abgelegt und ein weiterer Teil wird in einem freigegebenen (und replizierten) Laufwerk abgelegt, das „*SYSVOL-Ordner*“ genannt wird. Dieser Ordner ist auf allen Active Directory-Domänencontrollern vorhanden. Der Teil, der im Active Directory selbst gespeichert ist, wird „*Gruppen-Richtlinien-Container*“ (GPC) genannt. Der andere Teil, der im replizierten Ordner SYSVOL gespeichert wird, wird „*Gruppen-Richtlinien-Vorlage*“ (GPT) genannt.

Mit NT4-Clients wird die Richtlinien-Datei nur gelesen und ausgeführt, wenn der Benutzer sich am Netzwerk anmeldet. MS Windows 200x-Richtlinien sind wesentlich komplexer — GPOs werden beim Maschinenstart (maschinenspezifischer Teil) ausgeführt und zugewiesen, und bei der Benutzeranmeldung am Netzwerk wird der benutzerspezifische Teil zugewiesen. Bei einer Windows 200x-basierenden Richtlinien-Verwaltung kann jede Maschine und/oder jeder Benutzer Teil einer Anzahl von gleichzeitigen Anwendungen (und anwendbaren) Richtlinien-Sets (GPOs) sein. Active Directory erlaubt dem Administrator dabei auch Filter über die Richtlinien-Einstellungen zu setzen. Eine vergleichbare Möglichkeit existiert in NT4-basierenden Richtlinien-Dateien nicht.

22.2.3.1 Administration von Windows 200x/XP-Richtlinien

Anstatt das Werkzeug System-Richtlinien-Editor, gemeinhin auch Poledit genannt (nach dem Programmnamen **poledit.exe**), zu nutzen, werden GPOs durch Nutzung der Microsoft Management Console (MMC) erzeugt und verwaltet. Die Snap-Ins sind dabei folgende:

1. Gehen Sie in das Windows 200x/XP-Menü **Start->Programme->Administrations-Werkzeuge**, und suchen Sie nach dem MMC Snap-In **Active Directory Benutzer und Computer**.
2. Wählen Sie die Domäne oder Organisatorische Einheit (OU) aus, die Sie verwalten möchten. Dann klicken Sie mit der rechten Maustaste, um den Menükontext zu diesem Objekt aufzurufen, und suchen dann **Eigenschaften** heraus.
3. Klicken Sie mit der linken Maustaste auf den**Gruppen-Richtlinien**-Reiter, und klicken Sie dann auf **Neu**. Geben Sie einen Namen für die neue gewünschte Richtlinie ein, die Sie erzeugen möchten.
4. Klicken Sie mit der linken Maustaste auf **Bearbeiten** um die Schritte zur Erzeugung der GPO einzuleiten.

Alle Optionen zur Richtlinienkonfiguration werden durch die Nutzung der Vorlagen für die Administrationsrichtlinie kontrolliert. Diese Dateien haben die Endung .adm, sowohl bei NT als auch bei Windows 200x/XP. Achten Sie darauf, dass die .adm-Dateien nicht zwischen NT4 und Windows 200x austauschbar sind. Die zweite Möglichkeit beinhaltet eine Menge neuer Features und auch erweiterte Definitionsmöglichkeiten. Es ist jedoch nicht das Ziel dieser Dokumentation zu erklären, wie man .adm-Dateien programmiert; für diesen Zweck wird der Administrator auf das Microsoft Windows Resource Kit für die jeweilige MS Windows-Version verwiesen.

ANMERKUNG

Das MS Windows 2000 Resource Kit enthält ein Werkzeug namens `gpolmig.exe`. Dieses Werkzeug kann zur Migration einer NT4-NTConfig.POL-Datei in eine Windows 200x-GPO genutzt werden. Seien Sie SEHR vorsichtig bei der Nutzung dieses mächtigen Werkzeugs. Bitte ziehen Sie die Resource-Kit-Handbücher für weitergehende Informationen hinzu.

22.3 Zugriffs/Benutzer-Richtlinien verwalten

Richtlinien können bestimmte Benutzereinstellungen oder Einstellungen für eine Gruppe von Benutzern definieren. Die daraus entstehende Richtliniendatei enthält die Registry-Einstellungen für alle Benutzer, Gruppen und Maschinen, die die Richtliniendatei nutzen werden. Gesonderte Richtliniendateien für einzelne Benutzer, Gruppen oder Maschinen sind nicht mehr notwendig.

Falls Sie eine Richtlinie erzeugen, die automatisch von gültigen Domänencontrollern heruntergeladen werden soll, so müssen Sie den Dateinamen `NTConfig.POL` verwenden. Als Systemadministrator haben Sie durch Änderungen auf der Windows NT-basierenden Arbeitsstation die Möglichkeit, die Richtliniendatei umzubenennen, indem Sie die Maschine anweisen, die Aktualisierung der Richtlinien durch einen manuell eingegebenen Pfad durchzuführen. Sie können dies entweder durch manuelles Ändern der Registristrierungswerte tun oder durch Nutzung des System-Richtlinien-Editors. Es kann sogar ein lokales Verzeichnis sein, in dem die Machine Ihre eigene Richtliniendatei hat, aber wenn eine Änderung für alle Maschinen notwendig ist, muss diese an jeder Arbeitsstation durchgeführt werden.

Sobald eine Windows NT4/200x/XP-Maschine sich am Netzwerk anmeldet, sieht der Client in der NETLOGON-Freigabe des authentifizierten Domänencontrollers nach, ob die Datei `NTConfig.POL` existiert. Falls ja, wird diese heruntergeladen, durchgesehen und dann in den Benutzerteil der Registry eingelesen.

MS Windows 200x/XP-Clients, die sich an einer MS Windows-Active-Directory-Sicherheitsdomäne anmelden, werden ggf. zusätzliche Richtlinieneinstellungen durch Gruppen-Richtlinien-Objekte (GPOs) erwerben, die im Active Directory selbst abgespeichert sind. Die Hauptvorteile bei der Nutzung von AD-GPOs sind, dass diese keine *störenden* Effekte durchsetzen, die man in der Registry nicht brauchen kann. Dies hat beträchtliche Vorteile gegenüber der Nutzung von Richtlinien-Aktualisierungen, die auf `NTConfig.POL` im NT4-Stil basieren.

Zusätzlich zu Benutzerzugriffskontrollen, die durch System- und/oder Gruppen-Richtlinien in einer Weise durchgesetzt oder angewandt werden, die zusammen mit Benutzerprofilen arbeitet, erlaubt die Benutzerverwaltung unter MS Windows NT4/200x/XP sowohl eine Per-Domänen- als auch eine Per-Benutzer-Zugriffsverwaltung. Zu den allgemeinen Einschränkungen, welche häufig genutzt werden, zählen:

- Anmeldezeiten
- Passwortverfall
- Erlaubte Anmeldung nur von bestimmten Maschinen
- Zugriffstyp (lokal oder global)
- Benutzerrechte

Samba-3.0.0 hat nicht alle Zugriffskontrollen implementiert, die unter MS Windows NT4/200x/XP üblich sind. Während es möglich ist, viele Zugriffe durch Nutzung der Domänen-Benutzerverwaltung unter MS Windows NT4 zu setzen, ist derzeit nur der Passwortverfall implementiert. Die meisten der verbleibenden Kontrollen haben derzeit nur Subroutinen, die vielleicht einmal komplettiert werden, um alle Kontrollen zur Verfügung zu stellen. Vergessen Sie dabei aber auch nicht die Tatsache, dass Parameter auch durch Nutzung der NT4-Domänen-Benutzerverwaltung oder durch die Datei `NTConfig.POL` gesetzt werden können.

22.4 Verwaltungswerkzeuge

Jeder, der sich wünscht, Gruppen-Richtlinien erzeugen oder verwalten zu können, muss mit einer Reihe von Werkzeugen vertraut sein. Die folgenden Abschnitte beschreiben ein

paar der wichtigsten Werkzeuge, die Ihnen helfen werden, mit geringem Aufwand eine Benutzerumgebung anzulegen.

22.4.1 Der Samba-Werkzeug-Satz Editreg

Ein neues Werkzeug, **editreg** genannt, befindet sich derzeit in der Entwicklung. Dieses Werkzeug kann dazu genutzt werden, Registry-Dateien (`NTUser.DAT` genannt) zu bearbeiten, die in den Benutzer- und Gruppenprofilen enthalten sind. `NTConfig.POL`-Dateien haben diesselbe Struktur wie die Datei `NTUser.DAT` und können mit diesem Werkzeug bearbeitet werden. **editreg** wurde mit der Absicht geschrieben, `NTConfig.POL`-Dateien im Textformat abzuspeichern und die Erzeugung neuer `NTConfig.POL`-Dateien mit erweiterten Möglichkeiten zu gewährleisten. Es ist nachgewiesen, dass diese Möglichkeiten schwer zu realisieren sind, also seien Sie nicht überrascht, wenn Sie diese nicht gleich in die Tat umsetzen können. Offizielle Möglichkeiten werden zu dem Zeitpunkt publiziert, wenn das Werkzeug im Produktionsstadium ist.

22.4.2 Windows NT4/200x

Die Werkzeuge, die für diese Art der Verwaltung aus der MS Windows-Umgebung genutzt werden können, sind: der NT4-Benutzer-Manager für Domänen, der NT4-System- und Gruppen-Richtlinien-Editor und der Registry-Editor (regedt32.exe). Unter MS Windows 200x/XP kann dies mit der Microsoft Management Console (MMC) und geeigneten „*Snap-Ins*“ erfolgen, mit dem Registry-Editor und ggf. auch mit dem NT4 System- und Gruppen-Richtlinien-Editor.

22.4.3 Samba-PDC

In einem Samba-Domänencontroller sind die neuen Werkzeuge für die Benutzerzugriffsverwaltung und Richtlinien-Informationen enthalten: **smbpasswd**, **pdbedit**, **net** und **rpcclient**. Wenn Sie Administrator sind, sollten Sie die Manpages für diese Werkzeuge lesen und sich mit deren Bedienung vertraut machen.

22.5 Übersicht über den Systemstart und die Anmeldevorgänge

Die folgenden Zeilen versuchen die Reihenfolge zu erklären, in der System- und Benutzerrichtlinien durchgesetzt werden. Anschließend folgt ein Neustart des Systems und ein Teil einer Benutzeranmeldung:

1. Starten Sie das Netzwerk, dann den Remote Procedure Call System Service (RPCSS) und die Multiple Universal Naming Convention Provider (MUP).
2. Sobald Active Directory involviert ist, wird eine Liste von Gruppen-Richtlinien-Objekten (GPOs) heruntergeladen und ausgeführt. Diese Liste kann GPOs enthalten, die:
   - den Ort der Maschinen in einem Directory betreffen.
   - nur zutreffen, wenn Änderungen durchgeführt wurden.

- auf Einstellungen basieren, die die Anwendbarkeit von Möglichkeiten betreffen: lokal, Ort, Domäne, Organisatorische Einheit (OU) und so weiter.

Kein Benutzer-Desktop wird angezeigt, bevor Obiges nicht vollständig ausgeführt worden ist.

3. Ausführung von Startskripts (standardmäßig versteckt (hidden) und synchronisiert).
4. Eine Tastatureingabe-Aufforderung, um den Anmeldeprozess zu ermöglichen (Strg-Alt-Entf).
5. Benutzer-Referenzen werden geprüft und Benutzerprofile geladen (basierend auf den Richtlinien-Einstellungen).
6. Eine sortierte Liste von Benutzer-GPOs wird angezeigt?. Der Inhalt der Liste richtet sich danach, was hier konfiguriert wurde:
   - Ist der Benutzer ein Domänenmitglied oder Teil bestimmter Richtlinien ?
   - Loopback ist eingeschaltet und der Status der Loopback-Richtlinie (Zusammenführen oder Ersetzen).
   - Ort des Active Directory selbst.
   - Hat sich die Liste der GPOs geändert? Es ist keine Weiterverarbeitung notwendig, wenn nichts geändert wurde.
7. Benutzer-Richtlinien werden durch Active Directory durchgesetzt. Merke: Es gibt mehrere Arten.
8. Anmeldeskripten werden ausgeführt. Als Neuheit in Windows 200x und Active Directory können Anmeldeskripten beschafft werden, die auf Gruppen-Richtlinien-Objekten basieren (versteckt (hidden) und synchron ausgeführt). NT4-basierende Anmeldeskripten werden dann in einem normalen Fenster ausgeführt.
9. Das Benutzerinterface, das durch die GPOs bestimmt wurde, wird angezeigt. Merke: In einer Samba-Domäne (wie in jeder NT4-Domäne), werden Maschinen-(System-)Richtlinien beim Start durchgesetzt; Benutzer-Richtlinien werden beim Anmeldevorgang durchgesetzt.

22.6 Gängige Fehler

Mit Richtlinien verbundene Probleme können sehr schwer zu ermitteln und noch schwerer zu beheben sein. Die folgende Auswahl zeigt nur grundlegende Probleme.

22.6.1 Die Richtlinie arbeitet nicht

„*Wir haben die Datei* `Config.POL` *erzeugt und diese in der Freigabe* NETLOGON *abgespeichert. Es wurden keinerlei Änderungen an unseren Win XP Pro-Maschinen gemacht, wir sehen sie nicht einmal. Mit Windows 98 funktionierte dies prima, erst mit dem Update auf Win XP Pro nicht mehr. Ein paar Vorschläge?*“

Richtlinien-Dateien können nicht zwischen Windows 9x/Me- und MS Windows NT4/200x/XP-basierenden Plattformen ausgetauscht werden. Sie müssen den NT4-Gruppen-Richtlinien-Editor benutzen, um die Datei `NTConfig.POL` zu erzeugen, damit diese im richtigen Format für Ihre MS Windows XP Pro-Clients vorliegt.

Kapitel 23

DAS MANAGEMENT VON DESKTOP-PROFILEN

23.1 Eigenschaften und Vorzüge

So genannte „*Roaming Profiles*“ (zu Deutsch etwa „*servergespeicherte Benutzerprofile*“) werden von manchen gefürchtet, von einigen gehasst, von vielen geliebt und sind ein Geschenk des Himmels für so manchen Administrator.

Roaming Profiles erlauben es einem Administrator, dem Benutzer einen konsistenten Desktop zur Verfügung stellen, wenn er sich von einer Maschine zu einer anderen bewegt. Dieses Kapitel stellt Informationen darüber zur Verfügung, wie man Roaming Profiles konfiguriert und verwaltet.

Während Roaming Profiles für manche wie das Nirvana klingen mögen, sind sie für andere ein reales und konkretes Problem. Im Speziellen die Nutzer mobiler Computer, die oft keine dauerhafte Netzwerk-Verbindung haben, sind oft besser mit rein lokalen Profilen beraten. Dieses Kapitel bietet Informationen, um dem Samba-Administrator zu helfen, mit diesen Situationen umzugehen.

23.2 Roaming Profiles

> Warnung
>
> Die Unterstützung für Roaming Profiles ist für Windows 9x/Me und Windows NT4/200x unterschiedlich.

Bevor wir die Konfiguration von Roaming Profiles beschreiben, ist es sinnvoll zu sehen, wie Windows 9x/Me- und Windows NT4/200x-Clients diese Eigenschaften implementieren.

Windows 9x/Me-Clients senden einen „*NetUserGetInfo*“-Request an den Server, um den Pfad zu den Profilen des Benutzers zu erhalten. Die Antwort hat jedoch nicht genug Platz für ein separates Feld für den Pfad der Profile, nur für die home-Freigabe des Benutzers. Das bedeutet, dass Windows 9x/Me-Profile darauf beschränkt sind, im Home-Verzeichnis des Benutzers gespeichert zu werden.

Windows NT4/200x-Clients senden einen NetSAMLogon-RPC-Request, der viele Felder enthält, inklusive eines Feldes für den Pfad der Profile des Benutzers.

23.2.1 Die Konfiguration von Samba für den Umgang mit Profilen

Dieser Abschnitt dokumentiert, wie man Samba konfiguriert, um MS Windows-Client-Profile zu unterstützen.

23.2.1.1 NT4/200x-Benutzer-Profile

Um zum Beispiel Windows NT4/200x-Clients zu unterstützen, setzen Sie Folgendes im Abschnitt [global] der Datei `smb.conf`:

logon path = \\profileserver\profileshare\profilepath\%U\moreprofilepath

Dies wird typischerweise so implementiert: *logon path = \\%L\Profiles\%u*

wobei „*%L*“ in den Namen des Samba-Servers aufgelöst wird und „*%u*“ in den Benutzernamen.

Die Voreinstellung für diese Option ist `\\%N\%U\profile`, also `\\sambaserver\username\profile`. Der Dienst `\\%N\%U` wird automatisch vom [homes]-Dienst angelegt. Wenn Sie einen Samba-Server für die Profile verwenden, müssen Sie die in „*logon path*“ angegebene Freigabe durchsuchbar () machen. Bitte lesen Sie die Manpage für `smb.conf`, um mehr über die unterschiedliche Semantik von „*%L*“, „*%N*“, „*%U*“ und „*%u*“ zu erfahren.

> Anmerkung
>
>
>
> MS Windows NT/200x-Clients trennen manchmal zwischen einzelnen Logons eine Verbindung zu einem Server nicht. Es wird empfohlen, den Meta-Dienst *homes* nicht als Teil des Profil-Pfads zu verwenden.

23.2.1.2 Windows 9x/Me-Benutzer-Profile

Um Windows 9x/Me-Clients zu unterstützen, müssen Sie den Parameter logon home verwenden. Samba wurde repariert, so dass `net use /home` nun auch funktioniert und auch auf dem Parameter **logon home** beruht.

Durch die Verwendung des Parameters **logon home** sind Sie darauf beschränkt, Windows 9x/Me-Benutzer-Profile im home-Verzeichnis des Benutzers abzulegen. Aber warten Sie! Es

gibt einen Trick, den Sie benutzen können. Wenn Sie im Abschnitt *[global]* Ihrer `smb.conf`-Datei

```
logon home = \\%L\%U\.profiles
```

setzen, werden Ihre Windows 9x/Me-Clients pflichtbewusst ihre Profile in ein Unterverzeichnis Ihres home-Verzeichnisses namens `.profiles` ablegen (und sie damit verstecken).

Nicht nur das, `net use /home` wird aufgrund eines Features in Windows 9x/Me genauso funktionieren. Es entfernt jegliche Verzeichnis-Angaben am Ende der Angabe des home-Verzeichnisses und benutzt nur die Teile, die den Server und die Freigabe angeben. Daher sieht es für den Client so aus, als ob Sie `\\%L\%U` für logon home spezifiziert hätten.

23.2.1.3 Gemischte Windows 9x/Me- und Windows NT4/200x-Benutzer-Profile

Sie können Profile für Windows 9x/Me- und Windows NT4/200x-Clients unterstützen, indem Sie beide Parameter, logon home und logon path, angeben. Zum Beispiel:

```
logon home = \\%L\%u\.profiles
logon path = \\%L\profiles\%u
```

23.2.1.4 Die Unterstützung von Roaming Profiles deaktivieren

Oft wird gefragt: „*Wie kann ich die Verwendung lokaler Profile erzwingen?*“ oder: „*Wie kann ich Roaming Profiles deaktivieren?*“

Es gibt drei Arten, dies zu tun:

In `smb.conf` Ändern Sie die folgenden Settings, und ALLE Clients werden dazu gezwungen, ein lokales Profil zu verwenden: logon home und logon path.

MS Windows Registry Verwenden Sie die Microsoft Management Console gpedit.msc, um Ihre MS Windows XP- Maschine zu zwingen, nur ein lokales Profil zu verwenden. Dies verändert natürlich Registry-Settings. Der volle Pfad zu der Option ist:

```
Local Computer Policy\
   Computer Configuration\
      Administrative Templates\
         System\
            User Profiles\

Disable: Nur lokale Benutzer-Profile erlauben
Disable: Verhindern, dass Änderungen des Roaming Profile an den Server weitergegeb
```

Ändern des Profil-Typs: Klicken Sie im Start-Menü mit der rechten Maustaste auf **Arbeitsplatz**, wählen Sie **Properties**, klicken Sie auf das Tab **Benutzerprofile**, wählen

Sie das Profil, das Sie vom Typ **Roaming** auf **Local** ändern wollen, und klicken Sie auf **Typ ändern**.

Konsultieren Sie die Anleitung zur MS Windows Registry für Ihre spezifische Version von MS Windows, um mehr Informationen dazu zu erhalten, welche Registrierungsschlüssel zu ändern sind, um die Verwendung lokaler Benutzer-Profile zu erzwingen.

ANMERKUNG

Die Besonderheiten, wie man ein lokales Profil in ein Roaming Profil umwandelt oder umgekehrt, variieren je nach der Version von MS Windows, die Sie einsetzen. Konsultieren Sie auch das Microsoft MS Windows Resource Kit für besondere Informationen.

23.2.2 Informationen zur Konfiguration von Windows-Client-Profilen

23.2.2.1 Windows 9x/Me-Profil-Setup

Wenn sich ein Benutzer zum ersten Mal in Windows 9x anmeldet, werden die Datei user.DAT erstellt sowie die Verzeicnisse `Startmenü`, `Desktop`, `Programme` und `Netzwerkumgebung`. Diese Verzeichnisse und ihre Inhalte werden bei jedem folgenden Login mit den lokalen Versionen in `c:\windows\profiles\username` vereint, wobei immer die jeweils neuesten Versionen verwendet werden. Sie werden folgende *`[global]`*-Optionen verwenden müssen: preserve case = yes, short preserve case = yes und case sensitive = no, um Großbuchstaben in Shortcuts in einem der Profil-Verzeichnisse zu erhalten.

Die Datei `user.DAT` enthält alle Benutzereinstellungen. Wenn Sie einen Satz von Einstellungen erzwingen wollen, benennen Sie die Datei `user.DAT` in `user.MAN` um und verweigern den Schreibzugriff auf diese Datei.

1. Gehen Sie auf der Windows 9x/Me-Maschine auf **Systemsteuerung** -> **Passwörter**, und wählen Sie den Tab **Benutzer-Profile**. Wählen Sie das erforderliche Level von Roaming-Einstellungen. Drücken Sie **OK**, aber erlauben Sie keinen Reboot.

2. Dann gehen Sie auf **Systemsteuerung** ->, **Netzwerk** -> **Client for Microsoft Networks Einstellungen**. Wählen Sie **An NT Domäne anmelden**. Dann stellen Sie sicher, dass das Primary Logon **Client for Microsoft Networks** ist. Drücken Sie **OK**, und erlauben Sie diesmal den Reboot.

In Windows 9x/Me werden die Profile vom Primary Logon geladen. Wenn Sie das Primary Logon auf „*Client for Novell Networks*“ gesetzt haben, werden die Profile und Logon-Skripten vom Novell-Server geladen. Wenn Sie das Primary Logon auf „*Windows Logon*“ gesetzt haben, werden die Profile von der lokalen Maschine geladen, was ein wenig dem Prinzip der Roaming Profiles widerspricht, wie es scheint!

Sie werden nun sehen, dass der MS-Netzwerk-Login-Dialog `[Benutzer, Passwort, Domäne]` statt nur `[Benutzer, Passwort]` enthält. Geben Sie den Domänen-Namen des

Samba-Servers (oder den einer anderen existierenden Domäne, aber denken Sie daran, dass der Benutzer an dieser Domäne angemeldet wird und die Profile aus dieser Domäne geladen werden, wenn dieser Domänen-Anmelde-Server es unterstützt), den Benutzernamen und das Passwort des Benutzers ein.

Sobald der Benutzer erfolgreich überprüft wurde, wird die Windows 9x/Me-Maschine Ihnen Folgendes anzeigen: `The user has not logged on before` und Sie Folgendes fragen: `Do you wish to save the user's preferences?` Wählen Sie **Yes**.

Sobald der Windows 9x/Me-Client den Desktop hergestellt hat, sollte es Ihnen möglich sein, den Inhalt des im Parameter logon path angegebenen Verzeichnisses auf dem Samba-Server zu prüfen und festzustellen, dass die Ordner `Desktop`, `Startmenü`, `Programme` und `Netzwerkumgebung` angelegt worden sind.

Diese Ordner werden lokal auf dem Client gepuffert (Cache) und erfahren ein Update, wenn sich der Benutzer abmeldet (wenn Sie sie dann nicht schon auf read-only gesetzt haben). Sie werden sehen, dass der Client, wenn der Benutzer weitere Ordner oder Verknüpfungen anlegt, die heruntergeladenen Profil-Inhalte mit dem Inhalt des lokalen Profil-Ordners zusammenfügt, wozu er die neuesten Ordner und Verknüpfungen jeden Profil-Bestands verwendet.

Wenn Sie die Ordner/Dateien auf dem Samba-Server auf read-only gesetzt haben, werden Sie Fehler von der Windows 9x/Me-Maschine bei der An- und Abmeldung erhalten, wenn sie versucht, lokale und entfernte Profile zu vereinigen. Grundsätzlich sollten Sie die UNIX-Dateirechte und Eigentumsverhältnisse auf dem Samba-Server prüfen, wenn Sie irgendwelche Fehler von der Windows 9x/Me-Maschine erhalten.

Wenn Sie Probleme beim Anlegen von Benutzerprofilen haben, können Sie den lokalen Desktop-Cache des Benutzers zurücksetzen, wie unten gezeigt. Wenn sich dieser Benutzer das nächste Mal anmeldet, wird ihm gesagt werden, dass er/sie sich „*zum ersten Mal*“ anmeldet.

1. Anstatt sich im Dialog [Benutzer, Passwort, Domäne] anzumelden, drücken Sie **escape**.
2. Führen Sie **regedit.exe** aus, und suchen Sie nach:

   `HKEY_LOCAL_MACHINE\Windows\CurrentVersion\ProfileList`

   Sie werden einen ProfilePath-Eintrag für jeden Benutzer finden. Notieren Sie sich die Inhalte dieses Schlüssels (wahrscheinlich `c:\windows\profiles\username`), dann löschen Sie den Schlüssel *`ProfilePath`* für den erforderlichen Benutzer.
3. Verlassen Sie den Registry-Editor.
4. Suchen Sie nach der .PWL-password-caching-Datei des Benutzers im Verzeichnis `c:\windows`, und löschen Sie diese Datei.
5. Melden Sie sich vom Windows 9x/Me-Client ab.
6. Prüfen Sie die Inhalte des Profil-Pfads (siehe logon path, wie oben beschrieben), und löschen Sie die Datei `user.DAT` oder `user.MAN` des Benutzers, nachdem Sie, falls erforderlich, eine Sicherung angelegt haben.

> Warnung
>
> Bevor Sie die Inhalte des in *ProfilePath* angegebenen Verzeichnisses (wahrscheinlich `c:\windows\profiles\username`) löschen, fragen Sie den Benutzer, ob er irgendwelche wichtigen Dateien auf seinem Desktop oder im Startmenü gespeichert hat. Löschen Sie die Inhalte des Verzeichnisses *ProfilePath* (nach einem Backup, falls Dateien benötigt werden).
>
> Dies wird den Effekt haben, dass die lokale (read-only, versteckte) Datei `user.DAT` genauso wie die lokalen Ordner „*Desktop*“, „*Startmenü*“, „*Programme*“ und „*Netzwerkumgebung*“ aus dem Profil-Verzeichnis entfernt wird.

Wenn alles scheitert, erhöhen Sie Sambas Log-Level auf einen Wert zwischen 3 und 10 und/oder verwenden einen Packet-Sniffer wie ethereal oder **netmon.exe** und suchen nach Fehlermeldungen.

Wenn Sie Zugriff auf einen Windows NT4/200x-Server haben, installieren Sie zuerst Roaming Profiles und/oder Netzwerk-Anmeldungen auf dem Windows NT4/200x-Server. Führen Sie eine Paketverfolgung (Trace) aus, oder prüfen Sie die Beispiel-Traces, die dem Windows NT4/200x-Server beiliegen, und stellen Sie die Unterschiede zum Samba-Trace fest.

23.2.2.2 Windows NT4 Workstation

Wenn sich ein Benutzer zum ersten Mal an einer Windows NT4 Workstation anmeldet, wird das Profil `NTuser.DAT` angelegt. Der Ort, an dem das Profil abgelegt wird, kann durch den Parameter logon path angegeben werden.

Es gibt einen Parameter, der nun für die Verwendung mit NT-Profilen verfügbar ist: logon drive. Dieser sollte auf `H:` oder ein anderes Laufwerk gesetzt werden und in Verbindung mit dem neuen Parameter logon home verwendet werden.

Der Eintrag für das NT4-Profil ist ein Verzeichnis, keine Datei. Die NT-Hilfe bezüglich Profilen erwähnt, dass ein Verzeichnis auch mit der Endung .PDS angelegt wird. Der Benutzer muss beim Anmelden Schreibrechte haben, um den vollen Profil-Pfad anzulegen (und den Ordner mit der Endung .PDS, in den Fällen, in denen er angelegt wird).

Windows NT4 legt mehr Ordner im Profil-Verzeichnis an als Windows 9x/Me. So legt es den Ordner `Anwendungsdaten` und andere an, sowie `Desktop`, `Startmenü`, `Programme` und `Netzwerkumgebung`. Das Profil selbst wird in einer Datei namens `NTuser.DAT` gespeichert. Scheinbar wird nichts in dem Verzeichnis .PDS gespeichert, und sein Zweck ist uns momentan unbekannt.

Sie können die Systemsteuerung dazu verwenden, um ein lokales Profil auf einen Samba-Server zu kopieren (sehen Sie sich dazu die NT-Hilfe zu Profilen an; diese ist sogar dazu imstande, Sie zum richtigen Platz in der Systemsteuerung zu bringen). Die NT-Hilfe-Datei

erwähnt auch, dass das Umbenennen der Datei `NTuser.DAT` in `NTuser.MAN` ein Profil in ein zwingendes Profil verwandelt.

Die Groß-/Kleinschreibung des Profils ist wichtig. Die Datei muss `NTuser.DAT` heißen oder, für ein zwingendes Profil, `NTuser.MAN`.

23.2.2.3 Windows 2000/XP Professional

Sie müssen zuerst auf der MS Windows Workstation das Profil von einem lokalen Profil in ein Domänen-Profil umwandeln, und zwar wie folgt:

1. Melden Sie sich als der *lokale* Workstation-Administrator an.
2. Klicken Sie mit der rechten Maustaste auf das Icon **Arbeitsplatz**, und wählen Sie **Eigenschaften**.
3. Klicken Sie auf den Tab **Erweitert**.
4. Klicken Sie im Abschnitt **Benutzerprofile** auf den Eintrag **Einstellungen**.
5. Wählen Sie das Profil, das Sie umwandeln wollen (einmal darauf klicken).
6. Klicken Sie auf den Button **Kopieren nach**.
7. In der Box **Benutzer** klicken Sie auf **Ändern**.
8. Klicken Sie auf den Bereich **Pfade**, der den Maschinen-Namen listet; es wird sich eine Auswahl-Box öffnen. Klicken Sie auf die Domäne, für die das Profil zugänglich sein muss.

   ANMERKUNG

   Sie werden sich anmelden müssen, wenn sich ein Anmelde-Dialog öffnet. Zum Beispiel melden Sie sich an als *DOMÄNE*\root,passwort: *meinpasswort*.

9. Um einem Profil zu gestatten, von jedem verwendet zu werden, wählen Sie „*Jeder*“.
10. Klicken Sie auf **OK**; die Auswahl-Box schließt sich.
11. Nun klicken Sie auf **OK**, um das Profil im angegebenen Pfad anzulegen.

Erledigt. Sie haben nun ein Profil, das mit dem Samba-Tool **profiles** edititiert werden kann.

ANMERKUNG

Unter Windows NT/200x erzwingt die Verwendung von zwingenden Profilen die Verwendung von MS-Exchange für die Speicherung von Mail-Daten und hält diese außerhalb des Desktop-Profils. Dies verhindert, dass die Desktop-Profile unbenutzbar werden.

Windows XP Service Pack 1 Es gibt einen Sicherheits-Check, der neu für Windows XP ist (oder vielleicht nur für Windows XP Service Pack 1). Er kann über eine Gruppen-Richtlinie im Active Directory deaktiviert werden. Die Richtlinie heißt:

```
Computer Configuration\Administrative Templates\System\User Profiles\
Do not check for user ownership of Roaming Profile Folders
```

Dies sollte auf `Aktiviert` gesetzt werden.

Hat die neue Version von Samba ein Analogon zum Active Directory? Wenn ja, können Sie die Richtlinie eventuell durch dieses setzen.

Wenn Sie keine Gruppen-Richtlinien in Samba setzen können, dann können Sie sie vielleicht lokal auf jeder Maschine setzen. Wenn Sie dies versuchen wollen, machen Sie folgendes (Ich weiß nicht mit Sicherheit, dass dies genauso funktioniert wie eine Domänen-Gruppenrichtlinie):

1. Melden Sie sich auf der XP-Workstation mit einem Administrator-Konto an.
2. Klicken Sie auf **Start** -> **Ausführen**.
3. Geben Sie **mmc** ein.
4. Klicken Sie auf **OK**.
5. Eine Microsoft Management Console sollte erscheinen.
6. Klicken Sie auf **Datei** -> **Snap-In hinzufügen/entfernen** -> **Hinzufügen**.
7. Einen Doppelklick auf **Gruppenrichtlinie**.
8. Klicken Sie auf **Fertigstellen** -> **Schliessen**.
9. Klicken Sie auf **OK**.
10. In dem Fenster „*Konsolenstamm*“ klappen Sie **Richtlinien für Lokaler Computer** auf -> **Computerkonfiguration** -> **Administrative Vorlagen** -> **System** -> **Benutzerprofile**.
11. Einen Doppelklick auf **Eigentümer von servergespeicherten Profilen nicht prüfen**.
12. Wählen Sie **Aktiviert**.
13. Klicken Sie auf **OK**.
14. Schliessen Sie die gesamte Konsole. Sie müssen die Einstellungen nicht speichern (dies bezieht sich mehr auf die Konsolen-Einstellungen als auf die Richtlinien, die Sie geändert haben).

15. Rebooten Sie den Rechner.

23.2.3 Das gemeinsame Nutzen von Profilen mit Windows 9x/Me- und NT4/200x/XP-Workstations

Das gemeinsame Nutzen von Desktop-Profilen mit verschiedenen Windows-Versionen ist nicht zu empfehlen. Desktop-Profile sind ein Phänomen, das sich ständig weiterentwickelt, und Profile für spätere MS Windows-Versionen fügen Eigenschaften hinzu, die mit früheren MS Windows-Clients zu Problemen führen können. Der herausragendste Grund dafür, Profile nicht zu mischen, ist vermutlich folgender: Wenn man sich von einer älteren MS Windows-Version abmeldet, könnte das alte Format der Profil-Inhalte Informationen überschreiben, die zur neueren Version gehören, was zum Verlust von Profil-Informationsgehalt führt, wenn sich dieser Benutzer wieder an der neueren Version von MS Windows anmeldet.

Wenn Sie dasselbe Startmenü bzw. denselben Desktop mit W9x/Me teilen wollen, müssen Sie einen gemeinsamen Ort für die Profile angeben. Die Parameter in `smb.conf`, die gleich sein müssen, sind logon path und logon home.

Wenn Sie dies korrekt eingerichtet haben, werden Sie separate `user.DAT`- und `NTuser.DAT`-Dateien im selben Profil-Verzeichnis vorfinden.

23.2.4 Migration von Profilen von Windows NT4/200x Server zu Samba

Es gibt nichts, was Sie davon abhält, jeglichen beliebigen Pfad für die Benutzer-Profile anzugeben. Daher könnten Sie bestimmen, dass das Profil auf einem Samba-Server oder auf irgendeinem anderen SMB-Server gespeichert werden soll, solange dieser Server verschlüsselte Passwörter unterstützt.

23.2.4.1 Windows NT4-Werkzeuge zur Profil-Verwaltung

Leider sind die Informationen zum Resource Kit für die Version von MS Windows NT4/200x spezifisch. Das passende Resource Kit ist für jede Plattform erforderlich.

Hier eine Kurz-Anleitung:

1. Klicken Sie auf Ihrem NT4-Domänencontroller mit der rechten Maustaste auf **Arbeitsplatz**, dann wählen Sie den Tab namens **Benutzerprofile**.
2. Wählen Sie das Benutzerprofil, das Sie migrieren wollen, und klicken Sie darauf.

> ANMERKUNG
>
>
>
> Ich verwende den Begriff „*migrieren*“ nicht sehr streng. Sie können ein Profil kopieren, um ein Gruppen-Profil anzulegen. Sie können dem Benutzer *Jeder* Rechte an dem Profil geben, auf das Sie kopieren. Dies müssen Sie tun, da Ihre Samba-Domäne kein Mitglied einer Vertrauensstellung mit Ihrem PDC ist.

3. Klicken Sie auf **Kopieren nach**.
4. In dem Feld namens **Kopieren nach** geben Sie den neuen Pfad an, z.B., `c:\temp\foobar`
5. Klicken Sie auf **Ändern** im Feld **Benutzer**.
6. Klicken Sie auf die Gruppe „*Jeder*“, dann auf **OK**. Dies schliesst die Box „*Benutzer oder Gruppe wählen*“.
7. Jetzt klicken Sie auf **OK**.

Befolgen Sie obige Anleitung für jedes Profil, das Sie migrieren müssen.

23.2.4.2 Randbemerkungen

Sie sollten sich die SID Ihrer NT4-Domäne besorgen, dazu können Sie smbpasswd verwenden. Lesen Sie dazu die Manpage.

23.2.4.3 moveuser.exe

Das Windows 200x Professional Resource Kit enthält **moveuser.exe**. **moveuser.exe** verschiebt die Sicherheitseinstellungen eines Profils von einem Benutzer auf einen anderen. Dies erlaubt es, die Domäne des Kontos und/oder den Benutzernamen zu ändern.

Dieser Befehl ist dem Samba-Befehl **profiles** ähnlich.

23.2.4.4 Die SID erhalten

Sie können die SID bestimmen, indem Sie das Programm **GetSID.exe** aus dem Windows NT Server 4.0 Resource Kit verwenden.

Windows NT 4.0 speichert die lokalen Profil-Informationen an folgender Stelle in der Registry: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`

Im Schlüssel „*ProfileList*“ gibt es Sub-Schlüssel, die nach den SIDs der Benutzer benannt sind, die sich an diesem Computer angemeldet haben. (Um die Informationen zu dem Benutzer zu finden, dessen lokal zwischengespeichertes Profil Sie verschieben wollen, bestimmen Sie dessen SID mit dem Werkzeug **GetSID.exe**.) Innerhalb des entsprechenden Sub-Schlüssel des Benutzers werden Sie einen String-Wert namens *`ProfileImagePath`* finden.

23.3 Zwingende Profile

Ein zwingendes Profil („*Mandatory Profile*“) ist ein Profil, das der Benutzer nicht überschreiben kann. Während der einzelnen Sitzung des Benutzers sind Änderungen an der Desktop-Umgebung möglich, jedoch sind alle diese Änderungen beim Abmelden des Benutzers verloren. Wenn es erwünscht ist, dem Benutzer keinerlei Möglichkeit zur Veränderung der Desktop-Umgebung zu erlauben, muß dies durch Setzen von Richtlinien erfolgen. Lesen Sie dazu das vorhergehende Kapitel.

ANMERKUNG

Das Profil-Verzeichnis (oder dessen Inhalte) sollten unter KEINEN Umständen read-only gesetzt werden, da dies das Profil unbenutzbar machen kann. Wo es essenziell wichtig ist, ein Profil innerhalb des UNIX-Dateisystems read-only zu setzen, kann dies gemacht werden. In diesem Fall müssen Sie jedoch UNBEDINGT das VFS-Modul **fake-permissions** benutzen, um die MS Windows NT/200x/XP-Clients anzuweisen, dass der Benutzer Schreibberechtigung hat (siehe Abschnitt **??**).

Für MS Windows NT4/200x/XP kann die obige Methode auch zum Anlegen zwingender Profile verwendet werden. Um ein Gruppen-Profil in ein zwingendes Profil umzuwandeln, suchen Sie einfach nach der Datei `NTUser.DAT` im kopierten Profil und benennen sie in `NTUser.MAN` um.

Für MS Windows 9x/ME ist es die Datei `User.DAT`, die in `User.MAN` umbenannt werden muss, um ein zwingendes Profil zu erhalten.

23.4 Das Anlegen und Verwalten von Gruppen-Profilen

Die meisten Organisationen sind in Abteilungen gegliedert. Ein angenehmer Nebeneffekt dieser Tatsache ist, dass üblicherweise die meisten Benutzer innerhalb einer Abteilung dieselben Desktop-Anwendungen und dasselbe Desktop-Layout benötigen. MS Windows NT4/200x/XP erlaubt die Verwendung von Gruppen-Profilen. Ein Gruppen-Profil ist ein Profil, das ursprünglich unter Verwendung eines Beispiel-Anwenders angelegt wird. Danach werden unter Verwendung des Profil-Migrations-Tools (siehe oben) dem Profil Rechte für diejenige Benutzergruppe zugewiesen, die Zugriff auf das Gruppen-Profil benötigt.

Der nächste Schritt ist wichtig: Anstatt das Gruppen-Profil Benutzern auf einer „*per user*“-Basis zuzuweisen (mittels User Manager), wird die Gruppe selbst dem nunmehr modifizierten Profil zugewiesen.

ANMERKUNG

Seien Sie vorsichtig mit Gruppen-Profilen. Wenn der Benutzer, der Mitglied der Gruppe ist, auch ein persönliches Profil hat, wird das Ergebnis eine Vereinigung (Merge) dieser beiden Profile sein.

23.5 Standard-Profile für Windows-Benutzer

MS Windows 9x/Me und NT4/200x/XP benutzen ein Standard-Profil für jeden Benutzer, für den noch kein Profil existiert. Wenn man weiß, wo das Standard-Profil auf einer Windows-Workstation zu finden ist und welche Registrierungs-Schlüssel den Pfad beeinflussen, aus dem heraus das Standard-Profil angelegt wird, ist es möglich, das Standard-Profil für die jeweilige Installation zu optimieren. Dies hat signifikante administrative Vorteile.

23.5.1 MS Windows 9x/Me

Um Standard-Benutzer-Profile in Windows 9x/ME zu aktivieren, können Sie entweder den Windows 98 System Policy Editor verwenden oder die Registry direkt ändern.

Um Standard-Benutzer-Profile in Windows 9x/ME zu aktivieren, öffnen Sie den System Policy Editor, dann wählen Sie **Datei -> Registrierung öffnen**. Als Nächstes klicken Sie auf das Icon **Lokaler Computer**, klicken auf **Windows 98 System**, wählen **Benutzer-Profile** und klicken auf die Aktivieren-Box. Vergessen Sie nicht, die Registry-Änderungen zu speichern.

Zum direkten Modifizieren der Registry öffnen Sie den Registrierungs-Editor (**regedit.exe**) und wählen den Abschnitt `HKEY_LOCAL_MACHINE\Network\Logon`. Nun fügen Sie einen Wert vom Typ DWORD mit dem Namen „*User Profiles*“ hinzu. Um Benutzerprofile zu aktivieren, setzen Sie ihn auf 1; um diese zu deaktivieren, setzen Sie ihn auf den Wert 0.

23.5.1.1 Behandlung von Benutzerprofilen mit Windows 9x/Me

Wenn sich ein Benutzer an einer Windows 9x/Me-Maschine anmeldet, wird der lokale Profilpfad `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ProfileList` daraufhin überprüft, ob ein Eintrag für diesen Benutzer existiert.

Wenn der Benutzer einen Eintrag in diesem Registrierungsabschnitt hat, prüft Windows 9x/Me, ob eine lokal gepufferte Version des Benutzerprofils vorhanden ist. Windows 9x/Me prüft auch das Home-Verzeichnis des Benutzers (oder ein anderes angegebenes Verzeichnis, wenn diese Angabe verändert wurde) auf dem Server auf Vorhandensein des Profils. Wenn ein Profil an beiden Orten existiert, wird die neuere Version verwendet. Wenn das Benutzerprofil auf dem Server existiert, aber nicht auf der lokalen Maschine, wird das Profil vom Server geladen und verwendet. Wenn es nur auf der lokalen Maschine existiert, wird diese Kopie verwendet.

Wenn an keinem der beiden Orte ein Benutzerprofil gefunden wird, wird das Standard-Benutzer-Profil der Windows 9x/Me-Maschine verwendet und in einen neu angelegten Ordner für den angemeldeten Benutzer kopiert. Beim Abmelden werden alle vorgenommenen Änderungen des Benutzers in sein lokales Profil geschrieben. Wenn der Benutzer ein „*Roaming Profile*“ hat, werden die Änderungen in sein Profil auf dem Server geschrieben.

23.5.2 MS Windows NT4 Workstation

Unter MS Windows NT4 wird das Standard-Benutzer-Profil aus `%SystemRoot%\Profiles` bezogen, das in einer Standard-Installation `C:\Windows NT\Profiles` entspricht. Unter

diesem Verzeichnis gibt es in einer herkömmlichen sauberen Installation drei Verzeichnisse: `Administrator`, `All Users` und `Default User`.

Das Verzeichnis `All Users` enthält Menü-Einstellungen, die für alle System-Benutzer gleich sind. Das Verzeichnis `Default User` enthält Menü-Einträge, die - abhängig von den gewählten oder angelegten Profil-Einstellungen - an den jeweiligen Benutzer angepasst werden können.

Wenn sich ein neuer Benutzer zum ersten Mal an einer MS Windows NT4-Maschine anmeldet, wird ein neues Profil angelegt, das sich wie folgt zusammensetzt:

- All Users-Einstellungen
- Default User-Einstellungen (sie enthalten die Standard-Datei `NTUser.DAT`)

Wenn sich ein Benutzer an einer MS Windows NT4-Maschine anmeldet, die Mitglied einer MS-Domäne ist, werden die folgenden Schritte in Bezug auf Profile durchlaufen:

1. Die Information bezüglich des Benutzerkontos, die während dem Anmelde-Vorgang erhalten wird, enthält den Ort, an dem das Desktop-Profil des Benutzers aufbewahrt wird. Der Profil-Pfad kann lokal auf der Maschine liegen oder auf einer Netzwerk-Freigabe. Wenn ein Profil in dem vom Benutzer-Konto angegebenen Pfad existiert, wird es auf `%SystemRoot%\Profiles\%USERNAME%` kopiert. Dieses Profil erbt dann die Einstellungen im `All Users`-Profil in `%SystemRoot%\Profiles`.
2. Wenn das Benutzerkonto einen Profil-Pfad hat, aber dort kein Profil existiert, wird ein neues Profil in `%SystemRoot%\Profiles\%USERNAME%` angelegt. Dazu wird das Profil `Default User` verwendet.
3. Wenn die Freigabe NETLOGON auf dem authentifizierenden Server (Logon-Server) eine Richtlinien-Datei (`NTConfig.POL`) enthält, werden dessen Inhalte auf die Datei `NTUser.DAT` angewandt, die wiederum auf den Abschnitt `HKEY_CURRENT_USER` der Registrierung angewandt wird.
4. Beim Abmelden des Benutzers wird, wenn das Profil ein „*Roaming Profile*“ ist, das Profil in den Profil-Pfad geschrieben. Die Datei `NTuser.DAT` wird dann neu aus den Inhalten von `HKEY_CURRENT_USER` angelegt. Daher wird, falls beim nächsten Anmelden in der NETLOGON-Freigabe keine Datei `NTConfig.POL` existiert, die Auswirkung der vorigen Datei `NTConfig.POL` nach wie vor im Profil behalten. Diesen Effekt bezeichnet man als „*Tattooing*“.

MS Windows NT4-Profile können *lokal* oder *roaming* sein. Ein lokales Profil wird in `%SystemRoot%\Profiles\%USERNAME%` gespeichert. Ein „*Roaming Profile*“ wird auch in derselben Art gespeichert, es sei denn, der folgende Registrierungsschlüssel wird wie folgt angelegt:

```
HKEY_LOCAL_MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\winlogon\"Delet
```

In diesem Fall wird die lokale Kopie (in `%SystemRoot%\Profiles\%USERNAME%`) beim Abmelden gelöscht.

Unter MS Windows NT4 können Standard-Pfade für allgemeine Ressourcen wie `Eigene Dokumente` auf eine Netzwerk-Freigabe umgeleitet werden, indem man die folgenden

Registrierungs-Schlüssel ändert. Diese Änderungen können durch Verwendung des System Policy Editor vorgenommen werden. Dazu müssen Sie Ihre eigene Vorlage für den Policy Editor anlegen, um diese Änderungen per GUI zu erlauben. Eine andere Möglichkeit, dies zu tun, besteht darin, zuerst ein Standard-Benutzer-Profil anzulegen und dann, während man als anderer Benutzer angemeldet ist, **regedt32** auszuführen, um die Schlüssel zu editieren.

Der Registrierungsschlüssel, der das Verhalten der Ordner beeinflusst, die Teil des Standard-Benutzer- Profils sind, lautet unter Windows NT4:

```
HKEY_CURRENT_USER
   \Software
      \Microsoft
         \Windows
            \CurrentVersion
               \Explorer
                  \User Shell Folders
```

Der obige Schlüssel enthält eine Liste von automatisch verwalteten Ordnern. Die Standard-Einträge werde in Tabelle **??** gezeigt.

Tabelle 23.1. Standard-Werte der Registrierungsschlüssel für Benutzer-Ordner

Name	**Standard-Wert**
AppData	%USERPROFILE%\Anwendungsdaten
Desktop	%USERPROFILE%\Desktop
Favorites	%USERPROFILE%\Favoriten
NetHood	%USERPROFILE%\Netzwerkumgebung
PrintHood	%USERPROFILE%\Druckumgebung
Programs	%USERPROFILE%\Startmenü\Programme
Recent	%USERPROFILE%\Zuletzt verwendete Dokumente
SendTo	%USERPROFILE%\SendTo
Start Menu	%USERPROFILE%\Startmenü
Startup	%USERPROFILE%\Startmenü\Programme\Autostart

Der Registrierungsschlüssel, der den Ort der Standard-Profil-Einstellungen enthält, ist:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ User Shell Folders`

Die Standard-Einträge werden in Tabelle **??** gezeigt.

Tabelle 23.2. Standardwerte der Registrierungsschlüssel für Profil-Einstellungen

Gemeinsamer Desktop	%SystemRoot%\Profiles\All Users\Desktop
Gemeinsame Programme	%SystemRoot%\Profiles\All Users\Programme
Gemeinsames Startmenü	%SystemRoot%\Profiles\All Users\Startmenü
Gemeinsames Autostart	%SystemRoot%\Profiles\All Users\Startmenü\Programme\Startup

23.5.3 MS Windows 200x/XP

ANMERKUNG

MS Windows XP Home Edition verwendet standardmäßig Per-Benutzer-Profile, aber kann nicht an Domänen teilnehmen, sich nicht an NT/ADS-Domänen anmelden und kann daher das Profil nur von sich selbst beziehen. Während dies Vorteile hat, erlaubt es die „*Schönheit*" jener MS Windows-Clients, die an Domänen-Anmeldevorgängen teilnehmen können, dem Administrator, ein globales Standard-Profil anzulegen und dessen Verwendung mit Hilfe von Gruppenrichtlinien (GPOs) zu erzwingen.

Wenn sich ein neuer Benutzer zum ersten Mal an einer MS Windows 200x/XP-Maschine anmeldet, wird das Standard-Profil aus `C:\Dokumente und Einstellungen\Default User` geladen. Der Administrator kann die dortigen Inhalte modifizieren, und MS Windows 200x/XP wird diese verwenden. Dies ist nicht gerade optimal, da es bedeutet, dass man ein neues Standard-Profil auf jede MS Windows 200x/XP-Client-Workstation kopieren muss.

Wenn MS Windows 200x/XP an einem Domänen-Kontext teilnimmt und das Standard-Benutzer-Profil nicht gefunden wird, sucht der Client nach einem Standard-Profil in der NETLOGON-Freigabe des authentifizierenden Servers. In MS Windows-Begriffen handelt es sich um `%LOGONSERVER%\NETLOGON\Default User`, und wenn ein solches existiert, wird der Client es auf die Workstation kopieren, und zwar in das Verzeichnis `C:\Dokumente und Einstellungen\` unter dem Login-Namen des Benutzers.

ANMERKUNG

Dieser Pfad entspricht, in Samba-Begriffen, der Freigabe *`[NETLOGON]`* in `smb.conf`. Das Verzeichnis sollte im Wurzelverzeichnis dieser Freigabe angelegt werden und muss `Default Profile` heißen.

Wenn an diesem Ort kein Standard-Profil existiert, wird MS Windows 200x/XP das lokale Standard-Profil verwenden.

Beim Abmelden wird das Desktop-Profil des Benutzers an dem Ort abgespeichert, der in den Registrierungs-Einstellungen für diesen Benutzer gesetzt ist. Wenn keine spezifischen Richtlinien angelegt oder während der Anmeldung an den Client weitergegeben worden sind (wie es Samba automatisch tut), dann wird das Benutzerprofil nur auf der lokalen Maschine unter `C:\Dokumente und Einstellungen\%USERNAME%` abgelegt.

Jene, die dieses Standard-Verhalten verändern wollen, können dies auf drei Arten tun:

- Manuelles Ändern der Registrierungsschlüssel auf der lokalen Maschine und das Platzieren des Standard-Profils im Wurzelverzeichnis der NETLOGON-Freigabe. Dies wird nicht empfohlen, da es sehr wartungsintensiv ist.
- Anlegen einer NT4-artigen Datei `NTConfig.POL`, die dieses Verhalten spezifiziert, und das Platzieren dieser Datei im Wurzelverzeichnis der NETLOGON-Freigabe neben dem neuen Standard-Profil.
- Anlegen einer Gruppenrichtline (GPO), die das Verhalten per Active Directory erzwingt, und das Platzieren des neuen Standard-Profils in der NETLOGON-Freigabe.

Der Registrierungsschlüssel, der das Verhalten der Ordner beeinflusst, die Bestandteil des Standard-Benutzer-Profils sind, ist unter Windows 200x/XP:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\
```

Der obige Schlüssel enthält eine Liste von automatisch verwalteten Ordnern. Die Standard-Einträge werden in Tabelle **??** gezeigt.

Tabelle 23.3. Pfade des Standard-Profils: Standard-Werte der Registrierungsschlüssel

Name	**Standard-Wert**
AppData	%USERPROFILE%\Anwendungsdaten
Cache	%USERPROFILE%\Lokale Einstellungen\Temporary Internet Files
Cookies	%USERPROFILE%\Cookies
Desktop	%USERPROFILE%\Desktop
Favorites	%USERPROFILE%\Favoriten
History	%USERPROFILE%\Lokale Einstellungen\Verlauf
Local AppData	%USERPROFILE%\Lokale Einstellungen\Anwendungsdaten
Local Settings	%USERPROFILE%\Lokale Einstellungen
My Pictures	%USERPROFILE%\Eigene Dokumente\Eigene Bilder
NetHood	%USERPROFILE%\Netzwerkumgebung
Personal	%USERPROFILE%\Eigene Dokumente
PrintHood	%USERPROFILE%\Druckumgebung
Programs	%USERPROFILE%\Startmenü\Programme
Recent	%USERPROFILE%\Verlauf
SendTo	%USERPROFILE%\SendTo
Start Menu	%USERPROFILE%\Startmeüu
Startup	%USERPROFILE%\Startmenü\Programme\Autostart
Templates	%USERPROFILE%\Vorlagen

Es gibt auch einen Eintrag namens „*Default*“, der keinen Wert gesetzt hat. Der Standard-Eintrag ist vom Typ `REG_SZ`, alle anderen sind vom Typ `REG_EXPAND_SZ`.

Es macht einen riesigen Unterschied in Bezug auf die Geschwindigkeit, mit der man „*Roaming Profiles*“ verwenden kann, wenn all die notwendigen Ordner an einem dafür bestimmten Ort auf einem Netzwerk-Server abgelegt werden. Das bedeutet, dass es nicht

mehr notwendig ist, bei jedem An- und Abmelden die Outlook-PST-Datei über das Netzwerk zu schreiben.

Um dies auf einen Netzwerk-Pfad zu ändern, könnten Sie folgende Beispiele verwenden:

```
%LOGONSERVER%\%USERNAME%\Standard Ordner
```

Dies würde die Ordner im Home-Verzeichnis des Benutzers ablegen, und zwar in einem Ordner namens `Standard Ordner`. Sie könnten auch das verwenden:

*SambaServer**OrdnerFreigabe*\%USERNAME%

In diesem Fall werden die Standard-Ordner auf dem Server namens *SambaServer* in der Freigabe *OrdnerFreigabe* gespeichert, und zwar unter einem Verzeichnis, das den Namen des Windows-Benutzers hat, wie er vom Linux/UNIX-Dateisystem aus gesehen wird.

Bitte beachten Sie, dass Sie, sobald Sie eine Standard-Profil-Freigabe angelegt haben, das Benutzer-Profil darauf migrieren MÜSSEN (egal ob es ein Standard- oder angepasstes Profil ist).

MS Windows 200x/XP-Profile können *Local* oder *Roaming* sein. Ein „*Roaming Profile*“ wird lokal gepuffert (Cache), außer der folgende Registrierungsschlüssel wird angelegt:

```
HKEY_LOCAL_MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\
  winlogon\"DeleteRoamingCache"=dword:00000001
```

In diesem Fall wird die lokale Cache-Kopie beim Abmelden gelöscht.

23.6 Gängige Fehler

Im Folgenden werden typische Fehler, Probleme und Fragen beschrieben, die in den Samba-Mailing-Listen gestellt wurden.

23.6.1 Das Konfigurieren von „*Roaming Profiles*“ für einige wenige Benutzer oder Gruppen

Mit Samba-2.2.x haben Sie die Wahl, die Unterstützung von Roaming Profiles zu aktivieren oder zu deaktivieren. Die Voreinstellung ist, Roaming Profiles zu haben, und der Standard-Pfad wird diese im Home-Verzeichnis des Benutzers suchen.

Falls diese global deaktiviert sind, hat kein Benutzer die Fähigkeit, Roaming Profiles zu verwenden. Wenn diese aktiviert sind und Sie sie nur auf bestimmte Maschinen anwenden wollen, ist es notwendig, auf jenen Maschinen, die keine Unterstützung für Roaming Profiles bieten sollen, diese Unterstützung in der Registrierung jeder einzelnen dieser Maschinen zu deaktivieren.

Mit Samba-3 können Sie eine globale Profil-Einstellung in der `smb.conf` haben, und Sie können diese aufheben, indem Sie Per-Benutzer-Einstellungen mit dem Domain User Manager setzen (wie bei MS Windows NT4/ Win 200xx).

In jedem Fall können Sie nur ein Profil pro Benutzer konfigurieren. Dieses Profil kann sein:

- Ein Profil, das einzigartig für diesen Benutzer ist

- Ein zwingendes Profil (eines, das der Benutzer nicht ändern kann)
- Ein Gruppen-Profil (es sollte wirklich zwingend sein, also unveränderbar)

23.6.2 Ich kann keine Roaming Profiles verwenden

Ein Benutzer fragte Folgendes: „*Ich will keine Roaming Profiles implementieren. Ich möchte den Benutzern nur ein lokales Profil geben. Bitte helfen Sie mir, ich bin verloren ... Seit zwei Tagen versuche ich alles, google herum, aber finde keine hilfreichen Anhaltspunkte. Bitte um Hilfe!*“

Die Möglichkeiten sind:

Lokale Profile Ich kenne keine Registrierungseinstellungen, die das automatische Löschen von LOKALEN Profilen beim Abmelden erlauben.

Roaming Profiles Wenn sich ein Benutzer an einem Netzwerk anmeldet, wird ein zentral gespeichertes Profil auf die Workstation kopiert, um ein lokales Profil zu bilden. Dieses lokale Profil bleibt bestehen (verbleibt auf der Platte der Workstation), es sei denn, ein Registrierungsschlüssel wird geändert, der das automatische Löschen dieses Profils beim Abmelden veranlasst.

Die Möglichkeiten mit Roaming Profiles sind:

Persönliche Roaming Profiles Diese werden üblicherweise in einer Profil-Freigabe auf einem zentralen (oder einem praktisch gelegenen lokalen) Server gespeichert.

Workstations cachen (speichern) eine lokale Kopie des Profils. Diese gepufferte Kopie wird verwendet, wenn das Profil beim nächsten Anmelden nicht geladen werden kann.

Gruppen-Profile Diese werden von einem zentralen Profil-Server geladen.

Zwingende Profile Zwingende Profile können genauso für einen einzelnen Benutzer angelegt werden wie auch für jede Gruppe, deren Mitglied ein Benutzer ist. Zwingende Profile können nicht von einfachen Benutzern geändert werden. Nur der Administrator kann diese ändern oder neu konfigurieren.

Ein Windows NT4/200x/XP-Profil kann in seiner Größe variieren - von 130 Kbyte bis zu einem sehr großen Umfang. Outlook-PST-Dateien sind meistens Teil des Profils und können viele Gbyte groß sein. Im Durchschnitt (in einer gut verwalteten Umgebung) ist ein Roaming Profile von 2 Mbyte ein guter Richtwert für Planungszwecke. In einem undisziplinierten Umfeld habe ich bereits Profile von bis zu 2 Gbyte gesehen. Benutzer neigen dazu, sich zu beschweren, wenn es eine Stunde dauert, sich an einer Workstation anzumelden, jedoch ernten sie nur die Früchte von Unverstand (und Ignoranz).

Das bisher Erwähnte soll vor allem zeigen, dass Roaming Profiles, sowie eine gute Kontrolle darüber, wie diese verändert werden können, neben guter Disziplin wesentlich zu einer problemfreien Installation beitragen.

Microsofts Antwort auf das PST-Problem ist, alle E-Mail-Daten in einem MS Exchange Server-Backend zu speichern. Dies macht eine PST-Datei überflüssig.

Lokale Profile bedeuten:

- Wenn jede Maschine von vielen Benutzern verwendet wird, wird auch viel lokaler Speicherplatz für die Profile benötigt.
- Jede Workstation, an der sich der Benutzer anmeldet, hat ein eigenes Profil für ihn; diese Profile können sehr stark voneinander abweichen.

Auf der anderen Seite bedeutet der Einsatz von Roaming Profiles:

- Der Netzwerk-Administrator kann die Desktop-Umgebung aller Benutzer kontrollieren.
- Die Verwendung von zwingenden Profilen reduziert drastisch etwaige Overheads im Netzwerk-Management.
- Auf lange Sicht haben die Benutzer weniger Probleme damit.

23.6.3 Das Standard-Profil verändern

„*Wenn sich der Client am Domänen-Controller anmeldet, sucht er ein Profil zum Download. Wohin stelle ich dieses Standard-Profil?*“

Zuerst muss der Samba-Server als ein Domänen-Controller konfiguriert werden. Dies erfolgt durch Einstellungen in der `smb.conf`:

```
security = user
os level = 32 (or more)
domain logons = Yes
```

Es muss eine Freigabe namens *[netlogon]* geben, die world-readable ist. Es ist generell eine gute Idee, ein Start-Skript hinzuzufügen, das Drucker- und Laufwerksverbindungen vorbereitet. Es gibt außerdem eine Einrichtung zum automatischen Synchronisieren der Workstation-Uhr mit der des Anmelde-Servers (eine weitere gute Idee, dies zu verwenden).

ANMERKUNG

Um das automatische Löschen der Roaming Profiles aus dem lokalen Cache der Workstation (Festplatte) zu aktivieren, verwenden Sie den Group Policy Editor, mit dem Sie eine Datei namens `NTConfig.POL` mit den passenden Einträgen erstellen. Diese Datei muss im Wurzelverzeichnis der Freigabe *netlogon* platziert werden.

Windows-Clients müssen Domänen-Mitglieder sein. Arbeitsgruppen-Maschinen benutzen keine Netzwerk-Anmeldungen, also arbeiten sie auch nicht mit Domänen-Profilen zusammen.

Für Roaming Profiles fügen Sie Folgendes zur `smb.conf` hinzu:

```
        logon path = \\%N\profiles\%U
# Standard-Anmelde-Laufwerk ist Z:
        logon drive = H:
# Dies erfordert eine PROFILES-Freigabe, die world-writable ist.
```

Kapitel 24

PAM-BASIERTE VERTEILTE AUTHENTIFIZIERUNG

Dieses Kapitel hilft Ihnen, eine Winbind-basierende Authentifizierung auf jedem PAM-fähigen UNIX/Linux-System zu verwenden. Winbind kann verwendet werden, um eine Programm-Zugriffsauthentifizierung auf Benutzerebene von jeder MS Windows NT-Domäne, MS Windows 200x Active Director-basierenden Domäne oder einer Samba-basierten Domänen-Umgebung aus zu erlauben. Es sollte ihnen auch helfen, PAM-basierte lokale Host-Zugriffskontrollen zu konfigurieren, die Ihrer Samba-Konfiguration entsprechen.

Zusätzlich zur Konfiguration von Winbind in PAM werden Sie die PAM-Management-Möglichkeiten kennen lernen, wie z.B. die Verwendung von Werkzeugen wie `pam_smbpass.so`.

Anmerkung

Die Verwendung von Winbind erfordert mehr als nur die Konfiguration von PAM. Für mehr Informationen zu Winbind schauen Sie sich bitte Kapitel **??** „Winbind: Benutzung von Domänenkonten“ an.

24.1 Eigenschaften und Vorzüge

Eine Vielzahl von UNIX-Systemen (z.B. Sun Solaris) sowie die xxxxBSD-Familie und Linux benutzen inzwischen die Pluggable-Authentication-Modules-(PAM-)Dienste, um die gesamten Dienste für die Authentifikation, Autorisation und Ressourcen-Kontrolle anzubieten. Wollte man vor PAM eine Alternative zur systeminternen Passwortdatenbank (`/etc/passwd`) haben, musste man auch Änderungen oder Alternativen zu allen Programmen finden, die Sicherheitsdienste anbieten wie z.B. **login**, **passwd**, **chown** usw.

PAM liefert einen Mechanismus, der diese Sicherheitsprogramme von der darunterliegenden Authentifizierung/Autorisierung trennt. PAM wird konfiguriert, indem man Änderungen an

`/etc/pam.conf` vornimmt (Solaris) oder indem man die einzelnen Dateien, die in `/etc/pam.d` aufgelistet sind, anpasst bzw. verändert.

Auf PAM-fähigen UNIX/Linux-Systemen ist es ein einfaches Unterfangen, irgendein Authentifizierungs-Backend zu konfigurieren, solange die entsprechenden dynamisch ladbaren Modul-Bibliotheken vorhanden sind. Das Backend kann auf dem lokalen System oder zentralisiert, d.h. auf einem entfernten Server vorhanden sein.

PAM-unterstützte Module sind vorhanden für:

`/etc/passwd` Es gibt mehrere PAM-Module, die mit dieser Standard-UNIX-Benutzerdatenbank interagieren. Die bekanntesten sind `pam_unix.so`, `pam_unix2.so`, `pam_pwdb.so` und `pam_userdb.so`.

Kerberos Das Modul `pam_krb5.so` erlaubt die Nutzung von jedem Kerberos-fähigen Server. Dieses Tool kann mit MIT Kerberos, Heimdal Kerberos und möglicherweise mit Microsoft Active Directory (falls es eingeschaltet ist) benutzt werden.

LDAP Das `pam_ldap.so`-Modul erlaubt die Benutzung von jedem LDAP v2- oder LDAP v3-kompatiblem Backend-Server. Weit verbreitete LDAP-Backend-Server sind z.B. OpenLDAP v2.0 und v2.1, Sun ONE iDentity Server, Novell eDirectory Server und Microsoft Active Directory.

NetWare Bindery Das Modul `pam_ncp_auth.so` erlaubt die Authentifizierung auf jedem Bindery-fähigen NetWare-Core-Protokoll-basierenden Server.

SMB Password Dieses Modul, namentlich `pam_smbpass.so`, erlaubt die Benutzerauthentifizierung mit dem passdb-Backend, das in der Datei `smb.conf` angegeben ist.

SMB Server Das Modul `pam_smb_auth.so` ist das original MS Windows-Netzwerk-Authentifizierungs-Werkzeug. Dieses Modul ist eigentlich überholt, seit es das Winbind-Modul gibt.

Winbind Das Modul `pam_winbind.so` erlaubt Samba, sich an jedem MS Windows-Domänencontroller zu authentifizieren. Es kann genauso benutzt werden, um Benutzern den Zugang zu irgendeiner PAM-fähigen Applikation zu erlauben.

RADIUS Es gibt auch ein PAM-RADIUS-(Remote Access Dial-In User Service-) Authentifizierungsmodul. In den meisten Fällen muss der Administrator den Quellcode suchen und dieses Modul selbst kompilieren und installieren. RADIUS-Protokolle werden von vielen Routern und Terminalservern benutzt.

Von diesen Modulen stellt Samba nur das `pam_smbpasswd.so`- und das `pam_winbind.so`-Modul zur Verfügung.

Wenn sie einmal konfiguriert sind, erlauben diese Module einen bemerkenswerten Zuwachs an Flexibilität und die Benutzung von verteilten Samba-Domänencontrollern, die wiederum eine effiziente Ausnutzung der Bandbreite in großen Netzwerken mit PAM-fähigen Systemen erlauben. Richtig eingesetzt, erlaubt dies eine zentrale Administration einer verteilten Authentifizierung von einer Einzelbenutzer-Datenbank aus.

24.2 Technische Ausarbeitung

PAM wurde entworfen, um dem Systemverwalter eine große Flexibilität in der Konfiguration von Programmzugriffen auf das System zu geben. Die lokale Konfiguration der Systemsicherheit, die von PAM überwacht wird, liegt an einem dieser zwei Orte: entweder in der einzelnen System-Datei `/etc/pam.conf` oder im Verzeichnis `/etc/pam.d/`.

24.2.1 PAM-Konfigurationssyntax

In diesem Kapitel sehen wir uns die richtige Syntax und die verschiedenen Optionen der Einträge in diesen Dateien an. Bei PAM-spezifischen Zeichen ist die Groß- und Kleinschreibung egal. Bei den Modul-Pfaden hingegen spielt die Groß- und Kleinschreibung eine Rolle, da sie auf Dateinamen verweisen und diese die Schreibweise des Dateisystems wiedergeben. Ob bei den Argumenten der einzelnen Module auf die Groß- und Kleinschreibung geachtet werden muss, wird für jedes Modul eigens festgelegt.

Zusätzlich zu den unten beschriebenen Zeilen gibt es noch zwei zusätzliche Zeichen, die dem Systemadministrator die Arbeit erleichtern: Auszukommentierende Zeilen werden mit einem „#“ eingeleitet, das in der nächsten Zeile die Gültigkeit verliert; um Zeilen in einer Modulbeschreibung über den Zeilenumbruch zu verlängern, kann ein „\“ Zeichen verwendet werden.

Befindet sich das PAM-Authentifizierungsmodul (dynamisch ladbare Programmbibliothek) im Standardpfad, so ist es nicht nötig, den Pfad nochmals anzugeben. Befindet sich das Modul außerhalb dieses Pfades (unter Linux `/lib/security`), muss dieser wie folgt angegeben werden:

```
auth  required  /anderer_pfad/pam_fremdes_modul.so
```

24.2.1.1 Eigenschaften der Einträge in /etc/pam.d

Die restlichen Informationen in diesem Unterkapitel sind dem Linux-PAM-Dokumentationsprojekt entnommen. Für mehr Informationen zu PAM besuchen Sie diesen Link: The Official Linux-PAM home page. <`http://ftp.kernel.org/pub/linux/libs/pam/`>

Eine allgemeine Konfigurationszeile der Datei `/etc/pam.conf` hat folgende Form:

```
Service-name   Modul-type  control-flag   Modul-path  Args.
```

Hier beschreiben wir die Bedeutung dieser einzelnen Angaben. Bei der zweiten (und öfter angewendeten) Methode der Konfiguration von Linux-PAM ändern Sie den Inhalt des Ordners `/etc/pam.d/`. Nachdem wir die obigen Angaben erklärt haben, werden wir näher auf diese Methode eingehen.

Service-name Der Name des Dienstes, der mit diesem Eintrag verbunden ist. Meistens ist dies der herkömmliche Name der Anwendung. Zum Beispiel **ftpd**, **rlogind**, **su** usw.

Es gibt einen speziellen Dienste-Namen, der für einen Standard-Authentifizierungsmechanismus reserviert ist, und zwar den Namen *OTHER*, wobei es egal ist ob man ihn groß- oder kleinschreibt. Beachten Sie, dass dieser Parameter ignoriert wird, falls bereits ein Modul für einen Dienst namentlich angegeben ist.

module-type Einer von (momentan) vier Typen von Modulen, die da wären:

- *auth:* Dieser Modul-Typ stellt zwei Aspekte der Benutzerauthentifizierung zur Verfügung. Erstens wird festgestellt, dass der Benutzer der ist, der er angibt zu sein, indem er von der Applikation aufgefordert wird, ein Passwort anzugeben oder sich sonst irgendwie zu authentifizieren. Zweitens kann dieses Modul Gruppenzugehörigkeiten erlauben (unabhängig vom Inhalt von `/etc/groups`, der oben behandelt wurde) oder andere Privilegien, da es befähigt ist, diese zu vergeben.

- *account:* Dieses Modul führt ein nicht-authentifizierungsbasiertes Benutzermanagement aus. Normalerweise wird es benutzt, um den Zugang zu Diensten aufgrund der Tageszeit, der momentan verfügbaren Systemressourcen (maximale gleichzeitige Benutzer) oder vielleicht der Lage des „*root*“-Logins auf der Konsole zu erlauben oder verweigern.

- *session:* Dieses Modul wird vor allem verwendet, um festzulegen, was ausgeführt werden sollte, bevor ein Benutzer einen Dienst benutzt oder beendet. Dies könnte zum Beispiel das Aufzeichnen von Informationen bezüglich des Datenaustauschs mit dem Benutzer oder das Mounten von Ordnern usw. sein.

- *password:* Dieser letzte Modultyp wird gebraucht, um das mit dem Benutzer verbundene Authentifizierungstoken zu aktualisieren. Normalerweise gibt es ein Modul für jeden „*challenge/response*“ -basierten Authentifizierungs-*(auth)*-Modul-Typus.

control-flag Das control-flag wird benutzt, um festzulegen, wie die PAM-Bibliothek auf einen Erfolg oder Misserfolg des mit ihr verbundenen Moduls reagiert. Seit Module gestapelt werden können (Module des gleichen Typs werden nacheinander geschaltet, so dass eins nach dem anderen ausgeführt wird), legen die control-flags auch die relative Wichtigkeit dieser Module fest. Der Applikation wird nicht der Erfolg oder Misserfolg jedes Moduls in der `/etc/pam.conf`-Datei mitgeteilt, sondern sie erhält eine Zusammenfassung des Erfolgs oder Misserfolgs von der Linux-PAM-Bibliothek. Die Reihenfolge, in der diese Module ausgeführt werden, ist die der Einträge in `/etc/pam.conf`; der erste Eintrag wird als Erstes ausgeführt und der Letzte zum Schluss.

Ab Linux-PAM v0.60 kann dieses Control-flag mit einer von zwei Syntaxen angegeben werden.

Die einfachere (und historische) Syntax für das Control-flag ist ein einzelnes Schlüsselwort, das die Wichtigkeit des Erfolgs oder Misserfolgs des Moduls festlegt. Es gibt vier solcher Schlüsselwörter: *required, requisite, sufficient und optional*.

Die Linux-PAM-Bibliothek interpretiert diese Schlüsselwörter wie folgt:

- *required:* Dies gibt an, dass der Efolg dieses Moduls für den Erfolg des mit diesem Modul verbunden Dienstes wesentlich ist. Ein Misserfolg dieses Moduls wird dem Benutzer nicht mitgeteilt, bevor nicht alle anderen Module (desselben Modul-Typs) ausgeführt worden sind.

- *requisite:* Entspricht required, nur dass im Falle eines Misserfolges die Kontrolle direkt an die Applikation zurückgegeben wird. Der Rückgabewert ist der gleiche wie bei einem Misserfolg des ersten Moduls. Dieses Flag kann gesetzt werden, um dem Benutzer die Möglichkeit zu nehmen, das Passwort über ein unsicheres Medium einzugeben. Es wäre möglich, dass dies einem Angreifer Informationen über Benutzernamen geben könnte. Der Einsatz dieses Parameters sollte gut überlegt werden, da das nicht unerhebliche Risiko besteht, Passwörter in einer unsicheren Umgebung preiszugeben.

- *sufficient:* Der Erfolg dieses Moduls genügt, damit die Linux-PAM-Bibliothek ausgibt, dass dieses Modul erfolgreich war. In dem Fall, dass kein vorhergehendes wichtiges (*required*)-Modul einen Misserfolg zurückgab, wird kein weiteres „*gestapeltes*“ Modul ausgeführt (in diesem Fall werden auch keine weiteren wichtigen Module mehr ausgeführt). Ein Fehlschlagen dieses Moduls allein genügt nicht für das Fehlschlagen des Stapels.

- *optional:* Wie der Name schon sagt, bedeutet dieses Flag, dass das zugehörige Modul keinen kritischen Einfluss auf den Erfolg der Applikation des Benutzers hat. Wenn Linux-PAM festlegen muss, ob ein Modul-Stapel erfolgreich war, werden diese Module normalwerweise ignoriert. Sendet jedoch kein vorhergehendes oder nachfolgendes Modul des Stapels eine definitve Rückgabe über den Erfolg, ist der Rückgabewert dieses Moduls ausschlaggebend für den Erfolg des Modul-Stapels. Ein Beispiel für diesen Fall wäre, wenn die anderen Module eine Rückgabe wie PAM_IGNORE geben würden.

Die besser ausgearbeitete (und neuere) Syntax ist viel spezifischer und gibt dem Administrator mehr Möglichkeiten und Kontrolle darüber, wie der Benutzer authentifiziert wird. Diese Form der Kontroll-Flags wird mit eckigen Klammern abgegrenzt und besteht aus einer Serie von *value=action*-Paaren.

```
[value1=action1 value2=action2 ...]
```

Hier ist *value1* einer der folgenden Rückgabewerte:

```
success; open_err; symbol_err; service_err; system_err; buf_err;
perm_denied; auth_err; cred_insufficient; authinfo_unavail;
user_unknown; maxtries; new_authtok_reqd; acct_expired; session_err;
cred_unavail; cred_expired; cred_err; no_module_data; conv_err;
authtok_err; authtok_recover_err; authtok_lock_busy;
authtok_disable_aging; try_again; ignore; abort; authtok_expired;
module_unknown; bad_item; and default.
```

Der letzte dieser *(default)*-Parameter kann dafür benutzt werden, die Aktion für Rückgabewerte festzulegen, die nicht explizit definiert wurden.

Der Parameter *action1* kann ein positiver Integer-Wert oder eines der folgenden Zeichen sein: *ignore; ok; done; bad; die* und *reset*. Ein positiver Integer J kann, wenn er als Aktion festgelegt wurde, benutzt werden, um anzugeben, dass die nächsten J Module vom momentanen Modul-Stapel übersprungen werden sollen. Wird dies richtig angewendet, kann der Administrator einen hoch entwickelten Modul-Stapel mit mehreren Ausführungsmöglichkeiten bauen. Welche Möglichkeit letztendlich gewählt wird, kann mit der Reaktion der einzelnen Module bestimmt werden.

- *ignore:* Wird dieser Parameter mit in einem Modul-Stapel angewendet, beeinflusst die Rückgabe dieses Moduls nicht den Rückgabewert, den die Applikation vom gesamten Stapel erhält.
- *bad:* Dies gibt an, dass der Rückgabewert dieses Modul für das Fehlschlagen des Moduls ausschlaggebend ist. Wenn dieses Modul das erste ist, das erfolglos ausgeführt wird, wird sein Rückgabewert für den Status des gesamten Modul-Stapels verwendet.
- *die:* Das Gleiche wie *bad*, nur mit dem Effekt, dass der Modul-Stapel und PAM sofort abgebrochen werden und zur Anwendung zurückgekehrt wird.
- *ok:* Dieser Parameter teilt PAM mit, dass der Administrator glaubt, dieser Rückgabewert sollte direkt den Rückgabewert des gesamten Modul-Stapels beeinflussen. Mit anderen Worten: Wenn der vorherige Wert des Stapels einen Rückgabewert PAM_SUCCESS enthalten hätte, wird er jetzt von dem Rückgabewert dieses Moduls überschrieben. Achtung: Weist jedoch der vorherige Wert auf den Misserfolg eines Moduls hin, so wird der Parameter *ok* nicht verwendet, um diesen zu überschreiben.
- *done:* Das Gleiche wie *ok*, mit dem Effekt, dass der Modul-Stapel und PAM sofort beendet werden und zur Anwendung zurückgekehrt wird.
- *reset:* Löscht den Speicher des Rückgabewertes des Moduls und startet mit dem nächsten gestapelten Modul neu.

Jedes der vier Schlüsselwörter *required, requisite, sufficient* und *optional* hat einen gleichwertigen Ausdruck in der [...] Syntax:

- *required* entspricht *[success=ok new_authtok_reqd=ok ignore=ignore default=bad]*.
- *requisite* entspricht *[success=ok new_authtok_reqd=ok ignore=ignore default=die]*.

- *sufficient* entspricht *[success=done new_authtok_reqd=done default=ignore]*.
- *optional* entspricht *[success=ok new_authtok_reqd=ok default=ignore]*.

Um die Möglichkeiten im Umgang mit der neuen Syntax zu zeigen, folgen hier ein paar Beispiele. Mit Linux-PAM-0.63 wurde der Begriff „*Client Plug-in Agents*“ eingeführt. Dies macht es möglich, dass PAM eine Rechner-zu-Rechner-Authentifizierung erlaubt, die das Transportprotokoll der Client/Server-Applikation benutzt. Mit der Kontroll-Syntax *[... value=action ...]* kann eine Applikation so konfiguriert werden, dass sie binäre Aufforderungen entsprechender Clients unterstützt, jedoch ohne Probleme ältere Applikationen mit einer alternativen Methode authentifizieren kann.

module-path Der Pfadname der dynamisch ladbaren Objekt-Datei; das Plug-in-Modul selbst. Ist das erste Zeichen des Modulpfades ein „/“, wird davon ausgegangen, dass es ein absoluter Pfad ist. Ist dies nicht der Fall, wird der angegebene Pfad an den Standard-Modul-Pfad angehängt: `/lib/security` (siehe oben).

Die Argumente sind eine Liste von Zeichen, die an das Modul weitergegeben werden, wenn es aufgerufen wird. Sie sind damit den Argumenten eines normalen Linux-Shell-Befehls sehr ähnlich. Normalerweise sind gültige Argumente optional und für das angegebene Modul spezifisch. Ungültige Argumente werden vom Modul ignoriert, es wird jedoch ein Fehler in Syslog(3) geschrieben. Eine Liste der verschiedenen Optionen sehen Sie im nächsten Abschnitt.

Wenn Sie ein Leerzeichen in ein Argument einfügen möchten, sollten Sie es mit eckigen Klammern umschließen, z.B.:

```
squid auth required pam_mysql.so user=passwd_query passwd=mada \
db=eminence [query=select user_name from internet_service where \
user_name=%u und password=PASSWORD(%p) und service=web_proxy]
```

Wird dies so angewendet, kann man das Zeichen „]“ in der Zeichenkette verwenden. Möchte man das Zeichen „]“ in der Zeichenkette haben, das die Argumentübergabe überlebt, sollten Sie „\]“ verwenden. Mit anderen Worten:

```
[..[..\]..]    -->   ..[..]..
```

Jede Zeile in einer der Konfigurationsdateien, die nicht richtig formatiert ist, wird sehr wahrscheinlich dazu führen, dass der Authentifizierungsprozess fehlschlägt. Ein dementsprechender Fehler wird in die System-Logs geschrieben, mit einem Aufruf in der Syslog(3).

24.2.2 Beispiel einer System-Konfiguration

Im Folgenden sehen Sie ein Beispiel der Konfigurationsdatei `/etc/pam.d/login`. In diesem Beispiel sind alle Optionen eingeschaltet, und es ist möglicherweise nicht brauchbar, weil zu viele Bedingungen gestapelt werden, bevor ein erfolgreicher Abschluss erlaubt wird. Im Wesentlichen kann man alle Bedingungen auskommentieren, außer den Aufruf `pam_pwdb.so`.

24.2.2.1 PAM: Original-Login-Konfiguration

```
#%PAM-1.0
# The PAM configuration file for the login service
#
auth         required    pam_securetty.so
auth         required    pam_nologin.so
# auth       required    pam_dialup.so
# auth       optional    pam_mail.so
auth         required    pam_pwdb.so shadow md5
# account    requisite   pam_time.so
account      required    pam_pwdb.so
session      required    pam_pwdb.so
# session    optional    pam_lastlog.so
# password   required    pam_cracklib.so retry=3
password     required    pam_pwdb.so shadow md5
```

24.2.2.2 PAM: Login mit Verwendung von pam_smbpass

PAM erlaubt die Verwendung von austauschbaren Modulen. Auf einem Beispiel-System sollten folgende Module verfügbar sein:

```
$/bin/ls /lib/security
```

```
pam_access.so    pam_ftp.so          pam_limits.so
pam_ncp_auth.so  pam_rhosts_auth.so  pam_stress.so
pam_cracklib.so  pam_group.so        pam_listfile.so
pam_nologin.so   pam_rootok.so       pam_tally.so
pam_deny.so      pam_issue.so        pam_mail.so
pam_permit.so    pam_securetty.so    pam_time.so
pam_dialup.so    pam_lastlog.so      pam_mkhomedir.so
pam_pwdb.so      pam_shells.so       pam_unix.so
pam_env.so       pam_ldap.so         pam_motd.so
pam_radius.so    pam_smbpass.so      pam_unix_acct.so
pam_wheel.so     pam_unix_auth.so    pam_unix_passwd.so
pam_userdb.so    pam_warn.so         pam_unix_session.so
```

Das folgende Beispiel für das Login-Programm ersetzt die Verwendung des Moduls `pam_pwdb.so`, das die System-Passwort- Datenbank (`/etc/passwd`,`/etc/shadow`, `/etc/group`) mit dem Modul `pam_smbpass.so` benutzt, das die Samba-Datenbank verwendet, die die mit Microsoft-MD4 verschlüsselten Passwort- Hashes enthält. Diese Datenbank wird entweder in `/usr/local/samba/private/smbpasswd`, `/etc/samba/smbpasswd` oder in `/etc/samba.d/smbpasswd` aufbewahrt, je nach der Samba-Implementation Ihres UNIX/Linux-Systems. Das Modul `pam_smbpass.so` wird ab Samba-Version 2.2.1 mitgeliefert. Es kann mitkompiliert werden, indem man die Option `--with-pam_smbpass` einschaltet, wenn man Sambas **configure**-Skript aufruft. Mehr Informationen zum Modul `pam_smbpass` finden Sie in der Dokumentation im Ordner `source/pam_smbpass` der Samba-Quelldistribution.

```
#%PAM-1.0
# The PAM configuration file for the login service
#
auth        required    pam_smbpass.so nodelay
account     required    pam_smbpass.so nodelay
session     required    pam_smbpass.so nodelay
password    required    pam_smbpass.so nodelay
```

Folgendes ist eine PAM-Konfiguration für ein bestimmtes Linux-System. Unter Normalbedingungen wird `pam_pwdb.so` verwendet.

```
#%PAM-1.0
# The PAM configuration file for the samba service
#
auth       required     pam_pwdb.so nullok nodelay shadow audit
account    required     pam_pwdb.so audit nodelay
session    required     pam_pwdb.so nodelay
password   required     pam_pwdb.so shadow md5
```

Im folgenden Beispiel wurde die Entscheidung getroffen, die **smbpasswd**-Datenbank auch für Standard-Samba-Authentifizierungen zu verwenden. So eine Entscheidung könnte auch für das Programm **passwd** getroffen werden. Sie würde es erlauben, dass **smbpasswd**-Passwörter mit dem **passwd**-Programm geändert werden können.

```
#%PAM-1.0
# The PAM configuration file for the samba service
#
auth       required     pam_smbpass.so nodelay
account    required     pam_pwdb.so audit nodelay
session    required     pam_pwdb.so nodelay
password   required     pam_smbpass.so nodelay smbconf=/etc/samba.d/smb.conf
```

ANMERKUNG

PAM erlaubt das Stapeln von Authentifizierungsmechanismen. Es ist auch möglich, Informationen, die man in einem PAM-Modul erhalten hat, an das nächste Modul im PAM-Stapel weiterzugeben. Für Details zu den Fähigkeiten von PAM in Ihrem Umfeld, greifen Sie bitte auf die Dokumentation für Ihr spezifisches System zurück. Manche Linux-Implementationen enthalten ein Modul `pam_stack.so`, das es erlaubt, dass jede Authentifizierung in einer einzigen zentralen Datei konfiguriert wird. Die `pam_stack.so`-Methode hat einige Anhänger, da mit ihr eine einfachere Administration möglich ist. Wie so oft im Leben sind Entscheidungen mit Kompromissen verbunden, deshalb sollten Sie für mehr Informationen die PAM-Dokumentation konsultieren.

24.2.3 Die Konfiguration von PAM in smb.conf

Es gibt eine Option in `smb.conf`, die obey pam restrictions heißt. Folgendes findet man zu dieser Option in der Online-Hilfe von SWAT:

Wenn Samba mit PAM-Unterstützung konfiguriert wurde (`--with-pam`), gibt dieser Parameter an, ob Samba den PAM Konto- und Sitzungsrichtlinien gehorchen soll oder nicht. Das Standard-Verhalten sieht vor, dass PAM nur für die Klartext-Authentifizierung verwendet wird und dass das Konto- und Sitzungsmanagement ignoriert werden. Samba ignoriert PAM vollkommen, falls die Option encrypt passwords = yes hat. Dies ist so, weil PAM-Module nicht den challenge/response-Authentifizierungsmechanismus unterstützen, der von Samba bei der Passwort-Verschlüsselung verwendet wird.

Standard: obey pam restrictions = no

24.2.4 Entfernte CIFS-Authentifizierung mitwinbindd.so

Alle Betriebssysteme sind darauf angewiesen, dass Benutzerdaten so dargestellt werden, dass sie von der jeweiligen Plattform akzeptiert werden. UNIX benutzt dazu die Übergabe eines „*User Identifier*“ (UID) sowie eines „*Group Identifier*“ (GID). Dies sind beides Zahlen vom Typ Integer, die von einem Passwort-Backend wie `/etc/passwd` bezogen werden.

Benutzern und Gruppen unter Windows NT Server werden relative IDs (RID) zugeteilt, welche für die Domäne einzigartig sind, wenn der Benutzer oder die Gruppe erstellt wird. Um die Windows NT-Benutzer und -Gruppen in UNIX-Benutzer und -Gruppen umzuwandeln, ist ein Abgleich zwischen den RIDs und den UNIX-Benutzer- und -Gruppen-IDs erforderlich. Dies ist eine der Aufgaben, die Winbind ausführt.

So, wie Winbind-Benutzer und -Gruppen von einem Server aufgelöst werden, werden Benutzer- und Gruppen-IDs aus einer bestimmten Gruppe von Zahlen ermittelt. Diese werden auf einer Basis à la „*Wer zuerst kommt, kriegt zuerst*“ verteilt, obwohl alle bestehenden Benutzer und Gruppen gemappt werden, sobald ein Client einen Befehl zur Auflistung der

Benutzer und Gruppen gibt. Die zugeteilten UNIX-IDs werden in einer Datenbank-Datei im Samba-Lock-Verzeichnis gespeichert, um sie nachher wiederverwenden zu können.

Aufmerksame Administratoren werden bemerkt haben, dass die Kombination von `pam_smbpass.so`, **winbindd** und einem verteilten passdb backend wie *ldap* die Einrichtung einer zentral verwalteten, verteilten Benutzer/Passwort-Datenbank erlaubt, die von allen PAM-fähigen (d.h. Linux-) Programmen und Anwendungen verwendet werden kann. Dieses System kann große Vorteile im Vergleich zu Microsofts Active Directory Service (ADS) haben, da es den Authentifizierungsverkehr in großen Netzwerken reduziert.

WARNUNG

Die RID-zu-UNIX-ID-Datenbank ist der einzige Ort, an dem die Benutzer- und Gruppen-Umwandlung von **winbindd** gespeichert wird. Wenn diese Datei gelöscht oder beschädigt wird, hat **winbindd** keine Möglichkeit herauszufinden, welche Benutzer- und Gruppen-ID zu welcher Windows NT-Benutzer- oder Gruppen-RID gehört.

24.2.5 Passwort-Synchronisation mit pam_smbpass.so

`pam_smbpass` ist ein PAM-Modul, das auf entsprechenden Systemen dazu verwendet werden kann, die `smbpasswd`-(Samba-Passwort-)Datenbank mit der UNIX-Passwort-Datei laufend zu synchronisieren. PAM (Pluggable Athentication Modules) ist eine unter manchen UNIX-Betriebssystemen wie Solaris, HPUX und Linux unterstützte API, die den Authentifizierungsmechanismen eine generische Schnittstelle zur Verfügung stellt.

Dieses Modul authentifiziert eine lokale Benutzer-Datenbank `smbpasswd`. Wenn Sie die Authentifizierung auf einem entfernten SMB-Server benötigen oder wenn Sie über die Anwesenheit von SUID-root-Binärdateien auf Ihrem System besorgt sind, sollten Sie hingegen `pam_winbind` verwenden.

Die Optionen, die von diesem Modul akzeptiert werden, finden Sie in Tabelle **??**.

Im Folgenden sehen Sie ein paar Beispiele für die Anwendung von `pam_smbpass.so` im Format von Linux-`/etc/pam.d/`-Dateistrukturen. Möchte jemand dieses Werkzeug auch auf anderen Plattformen verwenden, muss er es passend adaptieren.

24.2.5.1 Konfiguration der Passwort-Synchronisation

Ein Beispiel einer PAM-Konfiguration, die die Verwendung von `pam_smbpass.so` zeigt, so dass `private/smbpasswd` mit `/etc/passwd (/etc/shadow)` synchronisiert bleibt, wenn diese verändert wird. Nützlich, wenn z.B. ein verfallenes Passwort möglicherweise von einem Programm geändert wird (z.B. **ssh**).

```
#%PAM-1.0
```

Tabelle 24.1. Gültige Optionen für pam_smbpass

debug	Mehr debug-Informationen werden aufgezeichnet.
audit	Das Gleiche wie debug, es werden aber zusätzlich noch unbekannte Benutzernamen geloggt.
use_first_pass	Den Benutzer nicht nach dem Passwort fragen, sondern diese aus den Elementen von PAM_ auslesen.
try_first_pass	Versuche, das Passwort von einem vorhergehenden PAM-Modul zu holen, Benutzer fragen.
use_authtok	Wie try_first_pass, aber *fail*, wenn die neue PAM_AUTHTOK nicht vorher gesetzt wurde(nur vorgesehen, um Password-Module zu stapeln).
not_set_pass	Passwörter, die dieses Modul verwendet, nicht für andere Module verfügbar machen.
nodelay	Keine Wartezeit von ~1 Sekunde bei Authentifizierungsfehlern.
nullok	Null-Passwörter sind erlaubt.
nonull	Null-Passwörter sind nicht erlaubt. Wird benutzt, um die Samba-Konfiguration zu übergehen.
migrate	Nur sinnvoll in einem „*auth*“-Kontext; wird benutzt, um die smbpasswd-Datei mit einem Passwort zu aktualisieren, das zu einer erfolgreiche Authentifizierung verwendet wurde.
smbconf=*file*	Legt einen alternativen Pfad zur Datei `smb.conf` fest.

```
# password-sync
#
auth       requisite    pam_nologin.so
auth       required     pam_unix.so
account    required     pam_unix.so
password   requisite    pam_cracklib.so retry=3
password   requisite    pam_unix.so shadow md5 use_authtok try_first_pass
password   required     pam_smbpass.so nullok use_authtok try_first_pass
session    required     pam_unix.so
```

24.2.5.2 Konfiguration der Passwort-Migration

Ein Beispiel einer PAM-Konfiguration, die die Verwendung von `pam_smbpass.so` zeigt, um von Klartext- zu verschlüsselten Passwörtern zu migrieren. Im Gegensatz zu anderen Methoden kann dies auch für Benutzer gemacht werden, die sich noch nie mit Samba-Freigaben verbunden haben: Die Passwort-Migration findet statt, sobald der Benutzer eine **ftp**-Verbindung herstellt, sich per **ssh** einloggt, seine Mails holt usw. ...

```
#%PAM-1.0
# password-migration
#
auth       requisite    pam_nologin.so
```

```
# pam_smbpass is called IF pam_unix succeeds.
auth       requisite   pam_unix.so
auth       optional    pam_smbpass.so migrate
account    required    pam_unix.so
password   requisite   pam_cracklib.so retry=3
password   requisite   pam_unix.so shadow md5 use_authtok try_first_pass
password   optional    pam_smbpass.so nullok use_authtok try_first_pass
session    required    pam_unix.so
```

24.2.5.3 Ausgereifte Passwort-Konfiguration

Das Folgende ist ein Beispiel einer Konfiguration für eine ausgereifte `smbpasswd`-Installation. `private/smbpasswd` ist mit Benutzern „*gefüllt*“, und wir betrachten es als Fehler, wenn kein SMB-Passwort vorhanden ist oder wenn es nicht mit dem UNIX-Passwort übereinstimmt.

```
#%PAM-1.0
# password-mature
#
auth       requisite    pam_nologin.so
auth       required     pam_unix.so
account    required     pam_unix.so
password   requisite    pam_cracklib.so retry=3
password   requisite    pam_unix.so shadow md5 use_authtok try_first_pass
password   required     pam_smbpass.so use_authtok use_first_pass
session    required     pam_unix.so
```

24.2.5.4 Konfiguration zur Integration von Kerberos-Passwörtern

Ein Beispiel einer PAM-Konfiguration, die die Verwendung von *pam_smbpass* zusammen mit *pam_krb5* zeigt. Dies kann für einen Samba-PDC nützlich sein, der zugleich Mitglied in einer Kerberos-REALM ist.

```
#%PAM-1.0
# kdc-pdc
#
auth       requisite   pam_nologin.so
auth       requisite   pam_krb5.so
auth       optional    pam_smbpass.so migrate
account    required    pam_krb5.so
password   requisite   pam_cracklib.so retry=3
password   optional    pam_smbpass.so nullok use_authtok try_first_pass
password   required    pam_krb5.so use_authtok try_first_pass
session    required    pam_krb5.so
```

24.3 Häufige Fehler

PAM kann sehr unbeständig und empfindlich gegenüber Ausrutschern bei der Konfiguration sein. Wir schauen uns hier ein paar Fälle aus der Samba-Mailingliste an.

24.3.1 pam_winbind-Problem

Ein Benutzer berichtet: Ich habe folgende PAM-Konfiguration:

```
auth required /lib/security/pam_securetty.so
auth sufficient /lib/security/pam_winbind.so
auth sufficient /lib/security/pam_unix.so use_first_pass nullok
auth required /lib/security/pam_stack.so service=system-auth
auth required /lib/security/pam_nologin.so
account required /lib/security/pam_stack.so service=system-auth
account required /lib/security/pam_winbind.so
password required /lib/security/pam_stack.so service=system-auth
```

Wenn ich mit [ctrl][alt][F1] eine neue Konsole aufmache, kann ich nicht mit meinem Benutzer „*pitie*“ einsteigen. Ich habe es auch mit dem Benutzer „*scienceu+pitie*“ versucht.

Antwort: Das Problem könnte an der Einbindung von *pam_stack.so service=system-auth* liegen. Diese Datei enthält oft eine Menge Zeilen, die Sachen doppelt machen, die man eigentlich schon tut. Versuchen Sie, die *pam_stack*-Zeilen für *auth* und *account* auszukommentieren, und probieren Sie es dann noch mal. Falls es so funktioniert, sollten Sie sich die Datei `/etc/pam.d/system-auth` ansehen und nur das Nötige in Ihre `/etc/pam.d/login`-Datei kopieren. Alternativ könnten Sie, wenn Sie für alle Dienste Winbind benutzen möchten, das Winbind-bezogene Material nach `/etc/pam.d/system-auth` verschieben.

24.3.2 Winbind löst Benutzer und Gruppen nicht auf

„*Meine* `smb.conf` *ist richtig konfiguriert. Ich habe Folgendes festgelegt: idmap uid = 12000 und idmap gid = 3000-3500;* ***winbind*** *läuft. Wenn ich Folgendes mache, funktioniert alles perfekt:*“

```
root# wbinfo -u
MITTELERDE+maryo
MITTELERDE+jackb
MITTELERDE+ameds
...
MITTELERDE+root

root# wbinfo -g
MITTELERDE+Domain Users
MITTELERDE+Domain Admins
MITTELERDE+Domain Guests
```

```
...
MITTELERDE+Accounts

root# getent passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
...
maryo:x:15000:15003:Mary Orville:/home/MITTELERDE/maryo:/bin/false
```

„*Aber folgender Befehl schlägt fehl:*“

```
root# chown maryo a_file
chown: 'maryo': invalid user
```

„*Das macht mich noch verrückt! Was könnte hier falsch sein?*“

Antwort: Auf Ihrem System läuft wahrscheinlich **nscd**, der „*name service caching daemon*“. Schalten Sie ihn aus, und starten Sie ihn nicht noch einmal! Dies sollte Ihr Problem lösen.

Kapitel 25

SAMBA IN MS-WINDOWS-NETZWERKE INTEGRIEREN

Dieses Kapitel handelt von der Auflösung von NETBIOS-TCP/IP-Namen in IP-Adressen. Wenn Ihre MS-Windows-Clients kein NetBIOS über TCP/IP verwenden, ist dieses Kapitel für Sie nicht relevant. Sollte Ihre Installation aber mit NetBIOS über TCP/IP arbeiten, kann Ihnen dieses Kapitel bei Netzwerkproblemen weiterhelfen.

ANMERKUNG

NetBIOS über TCP/IP hat nichts mit NetBEUI zu tun. NetBEUI ist NetBIOS über Logical Link Control (LLC). Bei aktuellen Netzwerken sollten Sie auf keinen Fall mehr NetBEUI verwenden. Es ist auch anzumerken, dass es nichts in der Art von NetBEUI über TCP/IP gibt. Wenn von so etwas gesprochen wird, handelt es sich um ein komplettes Missverständnis.

25.1 Fähigkeiten und Möglichkeiten

Viele MS-Windows-Netzwerkadministratoren hatten bisher keine Ahnung vom grundlegenden TCP/IP-Netzwerk-Betrieb, wie er in UNIX/Linux-Betriebssystemen verwendet wird. Andererseits haben viele Unix- und Linux-Administratoren keine Ahnung von den Komplikationen eines auf TCP/IP basierenden Windows-Netzwerks (und haben auch keinerlei Lust darauf ...).

Dieses Kapitel gibt für jede Betriebssystemumgebung eine kurze Einführung in die Grundlagen der Namensauflösung.

25.2 Hintergrundinformation

Seit der Einführung von MS Windows 2000 ist es möglich, ein MS-Windows- Netzwerk ohne NetBIOS über TCP/IP zu verwenden. NetBIOS über TCP/IP benutzt den UDP-Port 137 für die NetBIOS-Namensauflösung und den TCP-Port 139 für die NetBIOS-Dienste-Session. Sollte auf den MS Windows 2000-Clients (oder späteren Versionen) NetBIOS über TCP/IP deaktiviert sein, dann wird nur der TCP-Port 445 verwendet. In diesem Fall werden der UDP-Port 137 und der TCP-Port 139 nicht verwendet.

ANMERKUNG

Wenn Sie Windows 2000-Clients (oder neuere Versionen) verwenden und NetBIOS über TCP/IP nicht deaktiviert haben, benutzt der Client den UDP-Port 137 (NetBIOS Name Service, auch bekannt als Windows Internet Name Service oder WINS), den TCP-Port 139 und den TCP-Port 445 (für aktuellen Datei- und Druck-Verkehr).

Wenn Sie NetBIOS über TCP/IP deaktivieren, ist die Benutzung von DNS unumgänglich. Die meisten aktuellen Installationen, die NetBIOS über TCP/IP deaktivieren, verwenden MS Active Directory (ADS). ADS benötigt Dynamic DNS mit Service Resource Records (SRV RR) und Incremental Zone Transfers (IXFR). Die Benutzung von DHCP mit ADS wird für eine weitergehende zentrale Pflege der Netzwerkkonfiguration von Client-Workstations empfohlen.

25.3 Namensauflösung in einem reinen UNIX/Linux-Umfeld

Die wichtigsten Konfigurationsdateien in diesem Abschnitt sind:

- `/etc/hosts`
- `/etc/resolv.conf`
- `/etc/host.conf`
- `/etc/nsswitch.conf`

25.3.1 /etc/hosts

Diese Datei beinhaltet eine statische Liste von IP-Adressen und Namen.

```
127.0.0.1   localhost localhost.localdomain
192.168.1.1 bigbox.quenya.org bigbox   alias4box
```

Der Sinn der Datei `/etc/hosts` ist es, eine Möglichkeit zur Namensauflösung zu haben, damit Benutzer sich keine IP-Adressen merken müssen.

Netzwerk-Pakete, die über den Physical Network Transport Layer gesendet werden, kommunizieren nicht über die IP-Adresse, vielmehr wird die Media Access Control Address (auch MAC-Adresse genannt) verwendet. IP-Adressen sind zurzeit 32 Bit lang und werden typischerweise durch 4 dezimale und durch Punkte getrennte Zahlen dargestellt, zum Beispiel: 168.192.1.1

MAC-Adressen sind 48 Bit (oder 6 Byte) lang und werden typischerweise als zweistellige Hexadezimalziffern und durch Doppelpunkte getrennt dargestellt, zum Beispiel: 40:8e:0a:12:34:56

Jedes Netzwerkinterface muss eine MAC-Adresse besitzen. Einer MAC-Adresse können eine oder mehrere IP-Adressen zugeordnet sein. Es gibt keinen Zusammenhang zwischen einer MAC-Adresse und einer IP-Adresse; alle solche Zuweisungen sind beliebig frei und willkürlich. Auf der untersten Ebene der Netzwerkverbindungen wird die MAC-Adressierung verwendet. Da die MAC-Adresse global eindeutig und im allgemeinen fix für jedes einzelne Interface ist, macht die Zuordnung einer IP-Adresse nur aus Sicht des Netzwerkmanagements Sinn. Es kann mehr als eine IP-Adresse zu einer MAC-Adresse zugeordnet werden. Eine Adresse muss die primäre IP-Adresse sein. Diese Adresse wird bei einem ARP Reply zurückgegeben.

Wenn ein Benutzer oder ein Prozess mit einem anderen Computer kommunizieren will, stellt die Protokollschicht sicher, dass der „*Computername*“ oder „*Hostname*“ in eine IP- Adresse aufgelöst wird. Dies geschieht in der Art, wie es in den TCP/IP-Konfigurationsdateien hinterlegt ist. Die Datei `/etc/hosts` ist eine dieser Dateien.

Nachdem die IP-Adresse des Zielinterfaces ermittelt wurde, wird ein Protokoll mit dem Namen ARP/RARP verwendet, um die MAC-Adresse des Zielinterfaces herauszufinden. ARP bedeutet Address Resolution Protocol und ist eine broadcast-orientierte Methode, die über das User Data Protocol (UDP) eine Anfrage an alle Interfaces des lokalen Netzwerks verschickt. Netzwerkinterfaces sind so programmiert, dass sie nur auf zwei MAC-Adressen reagieren: auf ihre eigene eindeutige Adresse und auf die Adresse ff:ff:ff:ff:ff:ff. Die Antwort auf eine ARP-Anfrage enthält die MAC- Adresse und die primäre IP-Adresse für jedes Interface.

Die Datei `/etc/hosts` ist eine Grundvoraussetzung für alle UNIX/Linux-TCP/IP-Installationen und enthält als Minimum den localhost, die lokale IP-Adresse des Netzwerk-Interfaces und den primären Namen des lokalen Computers. Diese Datei hilft dabei, eine grundlegende Namensauflösung zu haben, bevor irgendwelche andere Methoden der Namensauflösung verfügbar sind.

25.3.2 /etc/resolv.conf

Diese Datei teilt den Bibliotheken zur Namensauflösung Folgendes mit:

- Den Namen der Domäne, zu der der Computer gehört.
- Die Namen der Domänen, die automatisch durchsucht werden, wenn die IP-Adresse zu einem unqualifizierten Rechnernamen gesucht werden soll.

- Den Namen oder die IP-Adresse der möglichen Domain-Name-Server, die für eine Namen-zu-Adressen-Übersetzung befragt werden können.

25.3.3 /etc/host.conf

`/etc/host.conf` ist primär dafür verantwortlich, wie die Einträge in `/etc/resolv.conf` beeinflusst werden. Es ist eine kritische Konfigurationsdatei, da hier die Reihenfolge der Namensauflösung eingestellt wird. Die typische Struktur sieht so aus:

```
order hosts,bind
multi on
```

Damit sollten beide Adressierungsarten verwendet werden. Für weitergehende Informationen werfen Sie bitte einen Blick in die Manpage für `host.conf`.

25.3.4 /etc/nsswitch.conf

Diese Datei kontrolliert die möglichen Ziele für eine Namensauflösung. Die Datei hat typischerweise folgende Spezifikationen für die Resolver-Objekte:

```
# /etc/nsswitch.conf
#
# Name Service Switch configuration file.
#

passwd:     compat
# Alternative entries for password authentication are:
# passwd:   compat files nis ldap winbind
shadow:     compat
group:      compat

hosts:      files nis dns
# Alternative entries for host name resolution are:
# hosts: files dns nis nis+ hesiod db compat ldap wins
networks:   nis files dns

ethers:     nis files
protocols:  nis files
rpc:     nis files
services:   nis files
```

Selbstverständlich muss sichergestellt sein, dass die zugehörigen Dienste und Einrichtungen für jeden dieser Mechanismen korrekt konfiguriert wurden.

Es sollte noch darauf hingewiesen werden, dass sich TCP/IP-Netzwerke still verhalten, solange keine Netzwerkanforderung/Nachricht verschickt werden muss. Bei allen TCP/IP-Verbindungen wird prinzipiell angenommen, dass sie sich nur bei Bedarf melden.

Seit Version 2.2.0 hat Samba Linux-Support für Erweiterungen der Name-Service-Switch-Infrastruktur. Darüber haben Linux-Clients die Möglichkeit, MS Windows-NetBIOS-Namen in IP-Adressen aufzulösen. Um diese Möglichkeit zu erhalten, muss Samba mit den passenden Parametern für das make-Kommando übersetzt werden (d.h. `make nsswitch/libnss_wins.so`). Die daraus entstehende Bibliothek sollte ins Verzeichnis `/lib` installiert werden, und der *wins*-Parameter muss zur Zeile „*hosts:*“ in der Datei `/etc/nsswitch.conf` hinzugefügt werden. Erst dann ist es möglich, jede MS Windows-Maschine über ihren NetBIOS-Computernamen anzupingen. Das geht aber nur, solange sich diese Maschine in derselben Arbeitsgruppe befindet.

25.4 Namensauflösung in einem MS Windows-Netzwerk

MS Windows-Netzwerke basieren auf den Namen, die jeder Computer erhält. Dieser Name wird auch oft (und uneinheitlich) als der „*Computer-Name,*“ „*Maschinen-Name,*“ „*Netzwerk-Name ,*“ „*NetBIOS-Name,*“ oder auch als „*SMB-Name*“ bezeichnet. Alle Begriffe meinen dasselbe, mit der Ausnahme vom „*NetBIOS-Name*“, denn dieser kann auch für den Namen der Arbeitsgruppe oder der Domäne verwendet werden. Die Begriffe „*Arbeitsgruppe*“ und „*Domäne*“ sind wirklich nur einfache Bezeichnungen für die Zugehörigkeit des Computers. Alle NetBIOS-Namen sind exakt 16 Zeichen lang. Das 16. Zeichen ist reserviert. Es wird benutzt, um einen 1 Byte langen Wert aufzunehmen, der die Service-Level-Informationen für den registrierten NetBIOS-Namen darstellt. Ein NetBIOS-Maschinen-Name ist daher für jeden angebotenen Service-Typ eines Client/Servers registriert.

Tabelle **??** und Tabelle **??** zeigen typische Registrierungen für NetBIOS-Namen und -Service-Typen.

Tabelle 25.1. Eindeutige NetBIOS-Namen

MASCHINENNAME<00>	Serverdienst läuft auf MASCHINENNAME
MASCHINENNAME<03>	Generischer Maschinenname (NetBIOS-Name)
MASCHINENNAME<20>	LanMan-Server-Dienst läuft auf MASCHINENNAME
ARBEITSGRUPPE<1b>	Domänen Master Browser

Tabelle 25.2. Gruppennamen

ARBEITSGRUPPE<03>	Generischer Name, registriert von allen Mitgliedern der ARBEITSGRUPPE
ARBEITSGRUPPE<1c>	Domänencontroller / Netlogon-Server
ARBEITSGRUPPE<1d>	Lokale Master Browser
ARBEITSGRUPPE<1e>	Dienst für Browser-Wahl

Es sei angemerkt, dass alle NetBIOS-Maschinen ihre eigenen Namen wie oben gezeigt registrieren. Das steht im krassen Gegensatz zu TCP/IP-Installationen, bei denen traditionell

der Systemadministrator in der `/etc/hosts` oder in der DNS-Datenbank festlegt, welche Namen mit welchen IP-Adressen verknüpft werden.

Ein weiterer Punkt sollte klargestellt werden: Die Datei `/etc/hosts` und die DNS-Einträge bieten keine Informationen zum NetBIOS-Namenstyp, die MS Windows-Clients benötigen, um den Typ des Dienstes zu finden. Sehen wir uns als Beispiel an, was passiert, wenn ein MS Windows-Client einen Domain-Logon-Server suchen möchte. Er findet diesen Service und die IP-Adresse des Servers, der diesen Dienst bietet, über einen NetBIOS-Broadcast und geht alle Maschinen durch, deren Namenstyp *<1c> ist. Anschließend wird ein Logon-Request an alle gefundenen IP-Adressen verschickt. Diejenige Maschine, die zuerst antwortet, führt dann den Logon-Prozess zu Ende.

Die Bezeichnung „*Arbeitsgruppe*“ oder „*Domain*“ kann sehr verwirrend sein, weil mit ihr eine zusätzliche Bedeutung verbunden ist, die die Sicherheitsarchitektur in MS Windows-Netzwerken beschreibt. Der Ausdruck „*Arbeitsgruppe*“ bezeichnet eine Netzwerkumgebung, die primär im Peer-to-Peer-Design aufgebaut ist. In einer Arbeitsgruppe sind alle Maschinen selbst für ihre eigene Sicherheit zuständig, und diese Sicherheit ist nur durch ein Passwort gewährleistet (das wird auch als „*Share Level Security*“ bezeichnet). In den meisten Peer-to-Peer-Netzwerken, in denen die Benutzer ihre eigenen Computer verwalten, wird keinerlei Sicherheit genutzt. Es ist in einer Arbeitsgruppen-Umgebung möglich, die User Level Security einzusetzen, dazu müssen aber ein Benutzername und ein zugehöriges Passwort verwendet werden.

MS Windows-Netzwerke sind darauf festgelegt, für die Verarbeitung der Nachrichten aller lokalen und fernen Computer Computernamen zu verwenden. Das verwendete Protokoll wird Server Message Block (SMB) genannt, und diese Implementierung verwendet das NetBIOS-Protokoll (Network Basic Input Output System). NetBIOS kann im LLC-Protokoll (Logical Link Control) verpackt sein. In diesem Fall wird das daraus resultierende Protokoll NetBEUI (Network Basic Extended User Interface) genannt. NetBIOS kann auch über IPX (Internetworking Packet Exchange), wie es Novell Netware benutzt, oder über das TCP/IP-Protokoll verwendet werden. Im letzten Fall wird das daraus resultierende Protokoll NBT oder NetBT genannt, also NetBIOS über TCPIP.

MS Windows-Computer verwenden eine Reihe von komplexen Mechanismen zur Namensauflösung. Da wir es primär mit TCP/IP zu tun haben, werden wir uns in dieser Dokumentation nur um diesen Bereich kümmern.

25.4.1 Der NetBIOS-Name-Cache

Alle MS Windows-Maschinen besitzen einen Speicherbereich, in dem sie die NetBIOS-Namen und IP-Adressen aller Maschinen speichern, mit denen sie in den letzten 10-15 Minuten Kontakt hatten. Es ist effizienter, bei einer Suche nach einer IP-Adresse zu einem Computer diese Information aus dem lokalen Cache zu erhalten, als alle konfigurierten Mechanismen zur Namensauflösung durchzugehen.

Wird eine Maschine, deren Name im lokalen Cache liegt, abgeschaltet, bevor der Eintrag ungültig geworden ist und bereinigt wurde, führt jeder Verbindungsversuch zu einer Time-Out-Verzögerung. Ist der Name im Cache, wird die Namensauflösung korrekt durchgeführt, aber die Maschine kann nicht antworten. Das kann die Bentutzer frustrieren, ist aber leider charakteristisch für dieses Protokoll.

Das MS Windows-Utility, das es ermöglicht, den NetBIOS-Cache zu überprüfen, wird „*nbtstat*“ genannt. Das Samba-Gegenstück wird **nmblookup** genannt.

25.4.2 Die Datei LMHOSTS

Diese Datei ist üblicherweise bei MS Windows NT 4.0 oder Windows 200x/XP im Verzeichnis `C:\WINNT\SYSTEM32\DRIVERS\ETC` zu finden und beinhaltet die Zuordnung der IP-Adressen zu den Computernamen. Die Datei `LMHOSTS` führt das NetBIOS-IP-Adressen-Mapping durch.

Sie sieht typischerweise in etwa so aus:

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Dies ist eine Beispieldatei für LMHOSTS, wie sie von Microsoft TCP/IP
# für Windows 2000 verwendet wird.
# Sie ist mit der LMHOSTS-Datei von Microsoft TCP/IP für LAN Manager 2.x
# kompatibel.
# Bearbeiten Sie diese Datei mit einem ASCII-Editor.
#
# In dieser Datei werden einzelnen IP-Adressen die entsprechenden
# Computernamen (NetBIOS-Namen) zugeordnet. Jeder Eintrag sollte aus
# einer einzelnen Zeile bestehen.
# Die IP-Adresse wird in der ersten Spalte eingetragen, gefolgt vom
# zugehörigen Computer-Namen. Die Adresse und der Computer-Name müssen
# dabei durch mindestens ein Leerzeichen oder ein Tabulatorzeichen
# getrennt sein.
# Das Zeichen "#" wird gewöhnlich Kommentaren vorangestellt. Ausnahmen
# hiervon sind die folgenden Erweiterungen:
#
#      #PRE
#      #DOM:<Domäne>
#      #INCLUDE <Dateiname>
#      #BEGIN_ALTERNATE
#      #END_ALTERNATE
#      \0xnn (Unterstützung nichtdarstellbarer Zeichen)
#
# Die Erweiterung "#PRE" wird nach dem Computer-Namen angegeben, wenn
# dieser Eintrag bereits zu Anfang in den Namen-Cache geladen werden
# soll. Standardmäßig werden die Einträge nicht zu Anfang in den Namen-
# Cache geladen, sie werden jedoch auch nur dann ausgewertet, wenn die
# dynamische Namensauswertung fehlschlägt.
#
# Die Erweiterung "#DOM:<Domäne>" wird nach dem Computer-Namen angegeben,
# wenn der Eintrag mit einer Domäne verknüpft werden soll.
# Dies wirkt sich auf das Verhalten des Computer-Suchdienstes und des
# Anmeldedienstes in der TCP/IP-Umgebung aus.
```

```
# Die Erweiterung "DOM:<Domäne>" kann zusammen mit der Erweiterung "PRE"
# für einen Eintrag angegeben werden.
#
# Die Angabe von "#INCLUDE <Dateiname>" veranlasst den NetBIOS Helper-
# Dienst die angegebene Datei zu suchen und sie wie eine lokale Datei
# auszuwerten. Für <Dateiname> werden UNC-Namen akzeptiert. Dadurch ist
# es möglich, eine LMHOSTS-Datei zentral auf einem Server zu verwalten.
# Befindet sich der Server außerhalb des Broadcast-Bereichs, ist eine
# Adresszuordnung für diesen Server vor der "#INCLUDE"-Anweisung not-
# wendig.
#
# Die Anweisungen "#BEGIN_ALTERNATE" und "#END_ALTERNATE" ermöglichen die
# Gruppierung von mehreren "#INCLUDE"-Anweisungen.
# Ist eine "INCLUDE"-Anweisung erfolgreich, werden alle weiteren
# "INCLUDE-ANWEISUNGEN" übersprungen und die Gruppe verlassen.
#
# Nichtdarstellbare Zeichen können im Computer-Namen enhalten sein.
# Solche Zeichen müssen als Hex-Wert in der \0xnn-Notation angegeben
# werden und zusammen mit dem NetBIOS-Namen in Anführungszeichen
# eingeschlossen werden.
#
#
# Beispiel:
#
# 102.54.94.97     maestro         #PRE #DOM:technik    # DC von "Technik"
# 102.54.94.102    "spiele \0x14"                       # besonderer Server
# 102.54.94.123    nordpol         #PRE                 # Server in 3/4317
# #BEGIN_ALTERNATE
# #INCLUDE \\lokal\public\lmhosts
# #INCLUDE \\maestro\public\lmhosts
# #END_ALTERNATE
#
# In diesem Beispiel enthält der Server "spiele" ein Sonderzeichen
# im Namen, und der Server "nordpol" wird bereits zu Anfang in den
# Namen-Cache geladen.
# Die Adresszuordnung für den Server "maestro" wird angegeben, um diesen
# Server weiter unten in der #INCLUDE-Gruppe verwenden zu können.
# Wenn der Server "lokal" nicht verfügbar ist, wird die zentrale LMHOSTS-
# Datei auf "maestro" verwendet.
#
# Beachten Sie, dass die gesamte Datei bei jeder Auswertung durchsucht wird,
# einschließlich der Kommentarzeilen. Es wird daher empfohlen, die obigen
# Kommentarzeilen zu entfernen.
```

25.4.3 Die Datei HOSTS

Diese Datei ist üblicherweise bei MS Windows NT 4.0 oder Windows 200x/XP im Verzeichnis `C:\WINNT\SYSTEM32\DRIVERS\ETC` zu finden und beinhaltet die IP-Adressen und IP-Namen- Paare. Sie kann von der Infrastruktur zur Namensauflösung in MS Windows verwendet werden, je nachdem, wie die TCP/IP-Umgebung konfiguriert wurde. Diese Datei ist in jeglicher Hinsicht das Gegenstück zur UNIX/LINUX-Datei `/etc/hosts`.

25.4.4 DNS-Lookup

Diese Möglichkeit wird im TCP/IP-Bereich der Netzwerkeinstellungen konfiguriert. Wenn sie eingeschaltet wurde, wird eine bestimmte Art der Namensauflösung verwendet, je nachdem, wie der NetBIOS-Node-Type-Parameter gesetzt ist. Ein Node Type 0 bedeutet, dass ein NetBIOS- Broadcast (über einen UDP-Broadcast) verwendet wird, falls die gewünschte Information einer Namensauflösung nicht im NetBIOS-Name-Cache gefunden worden ist. Wenn auch das fehlschlägt, werden DNS, HOSTS und LMHOSTS untersucht. Wenn der Node Type 8 eingestellt worden ist, dann wird eine Namensauflösung über NetBIOS-Unicast (über einen UDP-Unicast) zum WINS-Server versucht, bevor DNS, HOSTS, LMHOSTS oder ein Broadcast verwendet wird.

25.4.5 WINS-Lookup

Ein WINS-Service (Windows Internet Name Server) entspricht dem in RFC 1001/1002 spezifizierten NBNS (NetBIOS Name Server). Ein WINS-Server speichert die Namen und IP-Adressen, die Windows-Clients registrieren, wenn in deren TCP/IP-Setup mindestens eine WINS- Server-IP-Adresse angegeben wurde.

Um Samba als WINS-Server zu konfigurieren, muss folgender Parameter zur `smb.conf`-Datei hinzugefügt werden:

```
wins support = Yes
```

Um Samba für die Benutzung eines WINS-Servers zu konfigurieren, werden folgende Parameter in der `smb.conf` benötigt:

```
wins support = No
wins server = xxx.xxx.xxx.xxx
```

Dabei ist *xxx.xxx.xxx.xxx* die IP-Adresse des WINS-Servers.

Für Informationen über die Konfiguration von Samba als WINS-Server lesen Sie bitte Kapitel 10 „Netzwerk-Browsing“.

25.5 Häufige Fehler

Früher oder später findet jeder Netzwerkadministrator Probleme in der TCP/IP-Konfiguration. Die Ursachen können alles Mögliche sein, von Schreibfehlern über Vergesslichkeit, simplen Missverständnissen bis hin zu Achtlosigkeit. Aber niemand ist absichtlich achtlos!

25.5.1 Ping funktioniert nur in eine Richtung

„*Ich kann meinen Samba-Server von Windows aus anpingen, aber ich kann meine Windows-Maschine nicht von meinem Samba-Server aus anpingen.*“

Antwort: Die Windows-Maschine war unter der IP-Adresse 192.168.1.2 mit der Netzwerkmaske 255.255.255.0 zu erreichen, und der Samba-Server (Linux) war unter der IP-Adresse 192.168.1.130 mit der Netzwerkmaske 255.255.255.128 zu erreichen. Die Maschinen befinden sich in einem lokalen Netzwerk ohne externe Verbindungen.

Durch die inkonsistenten Netwerkmasken (die Windows-Maschine war im Netzwerk 192.168.1.0/24, während der Samba-Server im Netzwerk 192.168.1.128/25 war) sind das unterschiedliche Netzwerke.

25.5.2 Sehr langsame Netzwerkverbindungen

Gängige Ursachen von langsamen Netzwerkverbindungen können sein:

- Ein Client soll DNS benutzen, aber der DNS-Server ist heruntergefahren.
- Der Client soll einen Remote-DNS-Server benutzen, aber die Verbindung ist unterbrochen.
- Der Client soll einen WINS-Server benutzen, aber es gibt keinen WINS-Server.
- Der Client wurde ohne WINS konfiguriert, aber es gibt einen WINS-Server.
- Eine Firewall filtert unseren DNS- oder WINS-Verkehr.

25.5.3 Ein Problem bei der Namensänderung des Samba-Servers

„*Der Name des Samba-Servers wurde geändert, und Samba wurde neu gestartet. Der Samba-Server kann von Windows NT-Workstations nicht mit seinen neuen Namen angepingt werden, reagiert aber auf pings mit seinen alten Namen. Warum ?*“

Aufgrund der Beschreibung sind drei Dinge offensichtlich:

- WINS wird nicht verwendet, nur die broadcast-basierende Namensauflösung wird benutzt.
- Der Samba-Server wurde innerhalb der letzten 10-15 Minuten umbenannt und neu gestartet.
- Der alte Name des Samba-Servers ist noch im NetBIOS-Name-Cache der MS Windows-Workstation vorhanden.

Um herauszufinden, welche Namen noch im NetBIOS-Name-Cache des MS Windows NT4-Computers sind, öffnen Sie eine **cmd**-Kommandozeile und geben Folgendes ein:

```
C:\> nbtstat -n

            NetBIOS Local Name Table
```

```
   Name                 Type          Status
-------------------------------------------------
FRODO           <03>  UNIQUE      Registered
ADMINSTRATOR    <03>  UNIQUE      Registered
FRODO           <00>  UNIQUE      Registered
SARDON          <00>  GROUP       Registered
FRODO           <20>  UNIQUE      Registered
FRODO           <1F>  UNIQUE      Registered


C:\> nbtstat -c

            NetBIOS Remote Cache Name Table

   Name                 Type       Host Address     Life [sec]
-------------------------------------------------------------
GANDALF  <20>  UNIQUE      192.168.1.1          240

C:\>
```

Im obigen Beispiel ist GANDALF der Samba-Server und FRODO ist die MS Windows NT4-Workstation. Die erste Ausgabe zeigt den Inhalt der „*Local Name Table*“ (also die Identitätsinformationen der MS Windows-Workstation), und in der weiteren Ausgabe wird der NetBIOS-Name im NetBIOS-Name-Cache angezeigt. Der Name-Cache enthält die remote Computer, die diese Workstation kennt.

Kapitel 26

UNICODE/ZEICHENSÄTZE

26.1 Eigenschaften und Vorzüge

Wahrscheinlich wird jede Industrie erwachsen. Im Rückblick auf das letzte Jahrzehnt ist einer der wesentlichsten Bereiche dieses Erwachsenwerdens die Möglichkeit, dass jeder einen Computer bedienen kann. Das war nicht immer so, tatsächlich war es vor gar nicht allzu langer Zeit üblich, dass Software exklusiv für das Land geschrieben wurde, in dem sie verwendet werden sollte.

Von all den Anstrengungen, die unternommen wurden, um eine native Sprachunterstützung für alle Computer-Nutzer zur Verfügung zu stellen, ist den Anstrengungen der Openi18n-Organisation <`http://www.openi18n.org/`> besondere Beachtung zu schenken.

Samba-2.x unterstützte ein einzelnes Locale durch einen Mechanismus namens *codepages*. Samba-3 ist dazu bestimmt, eine echte transglobale Plattform für die Datei- und Druckerfreigabe zu werden.

26.2 Was sind Charsets und Unicode?

Computer kommunizieren in Zahlen. Jede Zahl wird in einen korrespondierenden Buchstaben übersetzt. Die Bedeutung, die einer entsprechenden Zahl zugeordnet wird, hängt vom genutzten *Character Set (Charset)* ab.

Ein Charset kann als Tabelle angesehen werden, die dazu verwendet wird, die Nummern in entsprechende Buchstaben umzuwandeln. (Es gibt unterschiedliche Charsets mit deutschen Umlauten, japanischen Zeichen usw.) Der „*American Standard Code for Information Interchange*“ (ASCII) war bis heute das maßgebliche Buchstaben-Schema, das von Computern verwendet wurde. ASCII ist ein Charset, das 128 Buchstaben darstellen kann. Die Verwendung dieser Kodierung bedeutet, dass jeder Buchstabe genau ein Byte groß ist.

Es gibt auch Charsets, die erweiterte Zeichen unterstützen, aber diese brauchen zumindest doppelt so viel Speicherplatz wie die ASCII-Kodierung. Solche Zeichensätze können **256 * 256 = 65.536** Zeichen enthalten, was mehr ist, als alle möglichen Zeichen, die man sich vorstellen kann. Diese Charsets werden Multibyte-Charsets genannt, weil sie mehr als ein Byte zum Speichern eines Zeichens verwenden.

Ein standardisiertes Multibyte-Charset ist als Unicode <http://www.unicode.org/> bekannt. Ein großer Vorteil bei der Verwendung eines Multibyte-Charsets ist, dass Sie nur eines brauchen. Man muss sich nicht mehr darum kümmern, dass zwei Computer dasselbe Charset verwenden, wenn sie miteinander kommunizieren.

Alte Windows-Clients verwenden Single-Byte-Charsets namens *Codepages* von Microsoft. Es gibt jedoch keine Unterstützung für das Aushandeln des Charsets im SMB/CIFS-Protokoll. Daher müssen Sie gewährleisten, dass Sie den richtigen Zeichensatz verwenden, wenn Sie mit einem älteren Client arbeiten. Neuere Clients (Windows NT, 200x, XP) verwenden bereits Unicode im Netzwerk.

26.3 Samba und Zeichensätze

Seit Samba-3 kann Samba Unicode über das Netzwerk verwenden (und tut es auch). Intern kennt Samba drei Typen von Zeichensätzen:

unix charset Dies ist der Zeichensatz, der intern von Ihrem Betriebssystem verwendet wird. Die Voreinstellung ist `UTF-8`, was passend für die meisten Systeme ist und alle Zeichen aller Sprachen abdeckt. Die Voreinstellung in älteren Samba-Versionen war `ASCII`.

display charset Dies ist der Zeichensatz, den Samba verwendet, um Meldungen auf Ihrem Bildschirm anzuzeigen. Er sollte allgemein derselbe sein wie *unix charset*.

dos charset Dies ist der Zeichensatz, den Samba verwendet, um mit DOS- und Windows 9x/Me-Clients zu kommunizieren. Mit allen neueren Clients wird Unicode gesprochen. Die Voreinstellung hängt von den auf Ihrem System installierten Zeichensätzen ab. Führen Sie **testparm -v | grep „*dos charset*“** aus, um den Standard-Zeichensatz auf Ihrem System angezeigt zu bekommen.

26.4 Konvertierung von alten Namen

Da vorhergehende Samba-Versionen keinerlei Zeichensatz-Konvertierung vorgenommen haben, sind die Zeichen in den Dateinamen üblicherweise im UNIX-Charset nicht korrekt, sondern nur im lokalen Zeichensatz, der von den DOS/Windows-Clients verwendet wird.

Bjoern Jacke hat ein Werkzeug namens convmv <http://j3e.de/linux/convmv/> geschrieben, das mit einem einzelnen Befehl ganze Verzeichnisstrukturen in andere Zeichensätze konvertiert.

26.5 Japanische Zeichensätze

Das Einrichten japanischer Zeichensätze ist ziemlich schwierig. Das liegt hauptsächlich an Folgendem:

- Der Windows-Zeichensatz ist nicht originalen japanischen Standard-Zeichensatz hinaus erweitert (JIS X 0208) und nicht standardisiert worden. Das bedeutet, dass die strikt standardisierte Implementierung nicht den vollen Windows-Zeichensatz unterstützen kann.
- Es gibt einige japanische Codierungsmethoden, die, hauptsächlich aus historischen Gründen, nicht vollständig kompatibel zueinander sind. Es gibt zwei Hauptcodierungen. Die eine ist die Serie Shift_JIS, die in Windows und einigen UNIX-Varianten verwendet wird; die andere ist die Serie EUC-JP, die in den meisten UNIX-Varianten und in Linux verwendet wird. Außerdem hat Samba früher auch einige einzigartige Codierungen namens CAP und HEX angeboten, um die Interoperabilität mit CAP/NetAtalk und UNIX-Varianten, die keine japanischen Dateinamen verwenden können, zu gewährleisten. Einige Implementationen der Serie EUC-JP unterstützen nicht den vollen Windows-Zeichensatz.
- Es gibt einige Umwandlungstabellen zwischen Unicode und überlieferten japanischen Zeichensätzen. Eine ist kompatibel mit Windows, eine andere basiert auf der Referenz des Unicode-Konsortiums, wieder andere sind gemischte Implementationen. Das Unicode-Konsortium definiert offiziell keine solchen Umwandlungstabellen, also kann es auch keine Standard-Tabelle geben.
- Der Zeichensatz und die Umwandlungstabellen, die in iconv() verfügbar sind, basieren auf der verfügbaren iconv-Library. Zusätzlich können sich die japanischen Locale-Namen auf den verschiedenen Systemen unterscheiden. Das bedeutet, dass der Wert der Zeichensatz-Parameter von der von Ihnen verwendeten Implementation von iconv() abhängt.

  Obwohl in Windows intern die Codierung „*2 byte fixed UCS-2*“ verwendet wird, wird in japanischen Umgebungen üblicherweise die Shift_JIS-Codierung so verwendet, wie in englischsprachigen Umgebungen ASCII.

26.5.1 Grundlegende Parameter-Einstellungen

dos charset und display charset sollten auf das Locale gesetzt werden, das kompatibel zu dem Zeichensatz und zu der Codierung ist, die unter Windows eingesetzt werden. Das ist üblicherweise CP932, hat aber manchmal einen anderen Namen.

unix charset kann entweder Shift_JIS, EUC-JP oder UTF-8 sein. UTF-8 ist immer verfügbar, aber die Verfügbarkeit anderer Locales und deren Namen hängen vom verwendeten System ab.

Sie können zusätzlich erwägen, die Serie Shift_JIS als Wert des Parameters unix charset zu verwenden, indem Sie das Modul vfs_cap verwenden, das dasselbe bewirkt wie das Setzen des Parameters „*coding system = CAP*“ in der Samba-Serie 2.2.

Wie man unix charset setzt, ist eine schwierige Frage. Die folgenden führt neben weitern Details die Vor- und Nachteile bei der Verwendung der verschiedenen Werte auf.

Shift_JIS-Serie Die Shift_JIS-Serie ist ein Locale, das äquivalent zu `Shift_JIS` ist und als Standard im japanischen Windows verwendet wird. Im Falle von `Shift_JIS` würde

ein Dateiname, der aus 0x8ba4 und 0x974c (einem japanisches 4-Byte-Zeichen, das „*Freigabe*“ bedeutet) und „*.txt*“ besteht und von Windows aus auf Samba geschrieben wird, unter UNIX zu 0x8ba4, 0x974c, „*.txt*“ werden (einem 8-Byte-Binär-String) wie unter Windows.

Die Shift_JIS-Serie wird üblicherweise in kommerziellen UNIX-Varianten, HP-UX und AIX als japanisches Locale verwendet. (Es ist jedoch auch möglich, die Serie EUC-JP zu verwenden.) Um die Shift_JIS-Serie auf diesen Plattformen zu verwenden, kann man die von Windows angelegten japanischen Dateinamen auch unter UNIX verwenden.

Wenn Ihr UNIX bereits mit Shift_JIS arbeitet und es einen Benutzer gibt, der japanische Dateinamen verwenden muss, die von Windows aus geschrieben werden, ist die Shift_JIS-Serie die beste Wahl. Es könnten jedoch beschädigte Dateinamen angezeigt werden, und einige Befehle, die nicht mit Nicht-ASCII-Dateinamen umgehen können, könnten bei der Analyse der Dateinamen abgebrochen werden. Insbesondere könnten „*\ (0x5c)*“ in Dateinamen vorkommen, mit denen besonders vorsichtig umgegangen werden muss. Also sind Sie besser beraten, Dateinamen, die von Windows auf UNIX geschrieben werden, nicht zu ändern.

Beachten Sie, dass die meiste freie Software, die „*japanisiert*“ wurde, nur mit EUC-JP funktioniert. Sie sollten prüfen, ob diese Software auch mit Shift_JIS funktioniert.

EUC-JP Serie Die EUC-JP-Serie entspricht einem Locale, das äquivalent zum Industrie-Standard EUC-JP ist, der in japanischem UNIX weit verbreitet ist (obwohl EUC auch Spezifikationen für andere Sprachen enthält, wie EUC-KR). Wenn Sie die EUC-JP-Serie einsetzen, würde ein japanischer Dateiname, der aus 0x8ba4 und 0x974c und „*.txt*“ besteht und von Windows auf Samba geschrieben wird, unter UNIX zu 0xb6a6, 0xcdad, „*.txt*“ werden (einem 8-Byte-Binär-String).

EUC-JP wird üblicherweise unter OpenSource-UNIX, Linux und FreeBSD als japanisches Locale verwendet und auf kommerziellem UNIX, Solaris, IRIX und Tru64-UNIX (obwohl es unter Solaris auch möglich ist, Shift_JIS und UTF-8 zu verwenden und unter Tru64-UNIX Shift_JIS). Um die EUC-JP-Serie zu verwenden, können die meisten japanischen Dateinamen, die von Windows angelegt wurden, auch unter UNIX verwendet werden. Außerdem arbeitet die meiste „*japanisierte*“ freie Software ausschließlich mit EUC-JP.

Es wird empfohlen, die Serie EUC-JP zu verwenden, wenn man japanische Dateinamen unter diesen UNIX-Varianten einsetzt.

Obwohl es kein Zeichen gibt, das ähnlich sorgfältig behandelt werden muss wie „*\ (0x5c)*“, können trotzdem beschädigte Dateinamen angezeigt werden, und einige Befehle, die nicht mit Nicht-ASCII-Dateinamen umgehen können, könnten bei der Analyse der Dateinamen abgebrochen werden.

Außerdem können, wenn Sie Samba mit einer anderen installierten libiconv kompiliert haben, das in libiconv enthaltene eucJP-ms-Locale und das im Betriebssystem enthaltene EUC-JP-Serien-Locale eventuell inkompatibel sein. In diesem Fall sollten Sie inkompatible Zeichen in Dateinamen vermeiden.

UTF-8 UTF-8 entspricht einem Locale, das äquivalent zu UTF-8 ist, dem internationalen Standard, der vom Unicode-Konsortium definiert wurde. In UTF-8 ist ein *Zeichen* durch 1-3 Bytes beschrieben. Im Falle von Japanisch werden die meisten Zeichen durch 3 Bytes beschrieben. Da unter Windows zur Darstellung von Japanisch Shift_JIS verwendet wird, wo ein Zeichen durch 1 oder 2 Bytes repräsentiert wird, wächst prinzipiell die Byte-Länge eines UTF-Strings auf die 1,5-fache Länge des originalen Shift_JIS-Strings an. Im Falle von UTF-8 wird ein japanischer Dateiname, der aus 0x8ba4, 0x974c und „*.txt*“ besteht und von Windows auf Samba geschrieben wird, unter UNIX zu 0xe585, 0xb1e6, 0x9c89, „*.txt*“ (einem 10-Byte-Binär-String).

Auf Systemen, wo iconv() nicht verfügbar oder inkompatibel zu Windows ist, ist UTF-8 das einzige verfügbare Locale.

Es gibt keine Systeme, die UTF-8 als voreingestelltes Locale für Japanisch benutzen.

Es könnten beschädigte Dateinamen angezeigt werden; und einige Befehle, die nicht mit Nicht-ASCII-Dateinamen umgehen können, könnten bei der Analyse der Dateinamen abgebrochen werden, besonders wenn „*\ (0x5c)*“ in Dateinamen vorkommen, womit vorsichtig umgegangen werden sollte. Also rühren Sie Dateinamen, die von Windows auf UNIX geschrieben wurden, besser nicht an.

Zusätzlich gilt (obwohl das nicht direkt mit Samba zu tun hat): Da es einen feinen Unterschied zwischen der Funktion iconv(), die allgemein unter UNIX verwendet wird, und den Funktionen auf anderen Plattformen wie Windows und Java gibt (was die Umwandlungstabelle zwischen Shift_JIS und Unicode betrifft), sollten Sie vorsichtig im Umgang mit UTF-8 sein.

Obwohl Mac OS X UTF-8 als seine Codierung für Dateinamen einsetzt, verwendet es eine erweiterte UTF-8-Spezifikation, mit der Samba nicht umgehen kann. Also ist das UTF-8-Locale nicht für Mac OS X verfügbar.

Shift_JIS Serie + vfs_cap (CAP-Codierung) Die CAP-Codierung ist eine Spezifikation, die in CAP und NetAtalk verwendet wird (beides sind Dateiserver für Macintosh-Rechner). Im Falle der CAP-Codierung wird ein japanischer Dateiname, der aus 0x8ba4, 0x974c und „*.txt*“ besteht und von Windows auf Samba geschrieben wird, unter UNIX zu „*:8b:a4:97L.txt*“ (einem 14-Byte-ASCII-String).

In der CAP-Codierung wird ein Byte, das nicht als ASCII-Zeichen dargestellt werden kann (0x80 oder höher), als „*:xx*“ codiert. Sie müssen darauf achten, „*\(0x5c)*“ in Dateinamen zu verwenden, aber die Dateinamen werden nicht beschädigt, wenn ein System nicht mit Nicht-ASCII-Dateinamen umgehen kann.

Der größte Verdienst der CAP-Codierung ist die Kompatibilität der Codierung mit CAP und NetAtalk. Da CAP und NetAtalk üblicherweise die Dateinamen auf UNIX mit CAP-Codierung schreiben, müssen Sie die CAP-Codierung einsetzen, wenn ein Verzeichnis sowohl mit Samba als auch mit NetAtalk freigegeben wird, um beschädigte Nicht-ASCII-Dateinamen zu vermeiden.

Es gibt jedoch einige Systeme, auf denen NetAtalk gepatcht wurde, um Dateinamen mit EUC-JP zu schrieben (z.B. japanisches Vine-Linux). Hier müssen Sie statt CAP EUC-JP verwenden.

vfs_cap selbst ist für Nicht-Shift_JIS-Locales verfügbar, die nicht mit Nicht-ASCII-Zeichen umgehen können, oder für Systeme, die Dateien mit NetAtalk freigeben.

Um die CAP-Codierung mit Samba-3 zu verwenden, sollten Sie den Parameter unix charset und VFS wie folgt verwenden:

Beispiel 26.5.1. VFS-CAP

```
[global]
        dos charset = CP932 Der Name des Locale CP932 könnte auch anders lauten
        unix charset = CP932
...

[cap-share]
        vfs option = cap
```

Sie sollten den Parameter unix charset auf CP932 setzen, wenn Sie GNU libiconv verwenden. Dadurch werden die Dateinamen in der Freigabe „*cap-share*“ mit CAP-Codierung geschrieben.

26.5.2 Individuelle Implementierungen

Dieser Abschnitt enthält noch zusätzliche Informationen zu individuellen Implementierungen:

GNU libiconv Damit libiconv sauber mit Japanisch umgeht, sollten Sie den Patch libiconv-1.8-cp932-patch.diff.gz <`http://www2d.biglobe.ne.jp/~msyk/software/libiconv-patch.html`> auf libiconv-1.8 anwenden.

Wenn Sie das gepatchte libiconv-1.8 verwenden, sind folgende Einstellungen verfügbar:

```
dos charset = CP932
unix charset = CP932 / eucJP-ms / UTF-8
      |       |
      |       +-- EUC-JP Serie
      +-- Shift_JIS Serie
display charset = CP932
```

Andere japanische Locales (z.B. Shift_JIS und EUC-JP) sollten wegen mangelnder Kompatibilität zu Windows nicht verwendet werden.

GNU glibc Damit die GNU glibc sauber mit Japanisch umgeht, sollten Sie den Patch <`http://www2d.biglobe.ne.jp/~msyk/software/glibc/`> auf glibc-2.2.5/2.3.1/2.3.2 anwenden oder die „*patch-merged*“-Versionen, glibc-2.3.3 oder später, einsetzen.

Bei der Verwendung der oben genannten glibc sind folgende Einstellungen verfügbar:

```
dos charset = CP932
unix charset = CP932 / eucJP-ms / UTF-8
display charset = CP932
```

Andere japanische Locales (z.B. Shift_JIS und EUC-JP) sollten wegen mangelnder Kompatibilität zu Windows nicht verwendet werden.

26.5.3 Migration von Samba-2.2

Vor den Samba-2.2-Releases wurde der Parameter „*coding system*“ wie der Parameter unix charset in Samba-3 verwendet. Tabelle **??** zeigt die Zuordnungstabelle, wenn man von Samba-2.2 auf Samba-3 migriert.

Tabelle 26.1. Japanische Zeichensätze in Samba-2.2 und Samba-3

Samba-2.2-Kodierungssystem	Samba-3-Unix-Charset
SJIS	Shift_JIS-Serie
EUC	EUC-JP-Serie
EUC3[a]	EUC-JP-Serie
CAP	Shift_JIS-Serie + VFS
HEX	derzeit kein Zeichensatz vorhanden
UTF8	UTF-8
UTF8-Mac[b]	derzeit kein Zeichensatz vorhanden
andere	derzeit kein Zeichensatz vorhanden

[a] Existiert nur in der japanischen Samba-Version
[b] Existiert nur in der japanischen Samba-Version

26.6 Gängige Fehler

26.6.1 CP850.so kann nicht gefunden werden

„*Samba beschwert sich über eine fehlende Datei* `CP850.so`.“

Antwort: CP850 ist die Voreinstellung für dos charset. Das dos charset wird zur Umwandlung von Daten in die Codepage verwendet, die Ihre DOS-Clients verwenden. Wenn Sie keine DOS-Clients haben, können Sie diese Meldung getrost ignorieren.

CP850 sollte von Ihrer lokalen iconv-Implementation unterstützt werden. Stellen Sie sicher, dass Sie alle erforderlichen Pakete installiert haben. Wenn Sie Samba aus dem Quelltext kompiliert haben, prüfen Sie, dass configure iconv gefunden hat.

Kapitel 27

BACKUP-TECHNIKEN

27.1 Eigenschaften und Vorzüge

Das Samba-Projekt ist nun über zehn Jahre alt. In der Frühzeit von Samba waren diejenigen, die es implementierten, meist UNIX-Administratoren. UNIX-Administratoren werden UNIX-Systemwerkzeuge verwenden, um UNIX-Systemdateien zu sichern. In den letzten vier Jahren interessiert sich eine stark zunehmende Anzahl von Microsoft-Netzwerk-Administratoren für Samba. Dies spiegelt sich in den allgemeinen Fragen zu Backups in den Samba-Mailinglisten wider.

27.2 Diskussion von Backup-Lösungen

Während einer Diskussion im Rahmen eines Microsoft Windows-Kurses erstaunte einer der Pro-UNIX-Teilnehmer die Klasse durch die Behauptung, dass Windows NT4 im Vergleich zu UNIX so limitierend sei. Er verglich UNIX mit einem Werkzeug-Set, das eine unbegrenzte Anzahl von Werkzeugen enthält, die simpel, effizient und, in Kombination verwendet, imstande seien, jegliches Ergebnis zu erzielen.

Eine Fürsprecherin des Windows-Networkings erwiderte, dass sie, wenn sie ein Werkzeug-Set haben wollte, eines kaufen würde. Sie betonte, dass sie ein einzelnes komplexes Werkzeug bevorzugen würde, das mehr tut als notwendig, dies jedoch mit einem klaren Zweck und Ziel.

Bitte beachten Sie, dass alle Informationen hier nur wiedergegeben werden, ohne Empfehlungen in Hinsicht auf Leistungsfähigkeit oder Angemessenheit. Als Netzwerk-Administrator sollten Sie unbedingt sorgfältige Recherchen durchführen, bevor Sie irgendeine Backup-Lösung implementieren, egal ob freie oder kommerzielle Software.

Eine nützliche Website, über die ich unlängst gestolpert bin, ist www.allmerchants.com <`http://www.allmerchants.com/Software/Backup_Software/`>. Sie sollten sie sich bei Gelegenheit ansehen.

Die folgenden freien Software-Projekte könnten auch Ihre Beachtung finden.

27.2.1 BackupPC

BackupPC in der Version 2.0.0 wurde auf SourceForge <`http://backuppc.sourceforge.net`> veröffentlicht. Neue Features beinhalten die Unterstützung von **rsync/rsyncd** und eine Internationalisierung der CGI-Oberfläche (einschließlich Englisch, Französisch, Spanisch und Deutsch).

BackupPC ist ein hoch-performantes Perl-basierendes Package zum Backup von Linux-, UNIX- oder Windows-PCs oder -Laptops auf die Festplatte eines Servers. Es ist hochgradig konfigurierbar, leicht zu installieren und zu warten. SMB (via smbclient), **tar** über **rsh/ssh** oder **rsync/rsyncd** werden zum Lesen der Client-Daten verwendet.

Angesichts der sinkenden Kosten von Festplatten und RAID-Systemen ist es nunmehr praktisch und kosteneffizient, eine große Anzahl von Maschinen auf die lokale Platte eines Servers oder dessen Netzwerk-Laufwerke zu sichern. Dies tut BackupPC.

Die Haupteigenschaften sind das „*Pooling*“ identischer Dateien (große Ersparnisse an Plattenplatz auf dem Server), Kompression und eine umfassende CGI-Oberfläche, die es Benutzern erlaubt, in Backups zu suchen und Dateien wiederherzustellen.

BackupPC ist freie Software, die unter der GNU GPL-Lizenz vertrieben wird. Es läuft auf Linux/UNIX/freenix-Servern und wurde auf Clients unter Linux, UNIX, Windows 9x/ME, Windows 98, Windows 200x, Windows XP und Mac OSX getestet.

27.2.2 Rsync

rsync ist ein flexibles Programm zum effizienten Kopieren von Dateien und Verzeichnisbäumen.

rsync hat viele Optionen, um auszuwählen, welche Dateien kopiert werden und wie sie übermittelt werden sollen. Es kann als Alternative zu **ftp, http, scp** oder **rcp** verwendet werden.

Das rsync „*remote-update*“-Protokoll erlaubt es dem Programm, nur die Unterschiede zwischen zwei Dateibeständen über das Netzwerk transportieren zu müssen. Dazu wird ein effizienter Prüfsummen-Such-Algorithmus verwendet, der in dem technischen Report beschrieben wird, der im rsync-Package enthalten ist.

Einige der zusätzlichen Features von rsync sind:

- Unterstützung für das Kopieren von Links, Geräte-Dateien, Benutzern, Gruppen und Berechtigungen
- Exclude- und exclude-from-Optionen ähnlich zu GNU tar
- Ein CVS-exclude-Modus, um dieselben Dateien zu ignorieren, die auch CVS ignoriert
- rsync kann jede transparente Remote Shell verwenden, inklusive rsh oder ssh.
- rsync erfordert keine root-Privilegien.
- Dateitransfers werden in Pipelines zusammengefasst, um Latenz zu minimieren.
- Unterstützung für anonyme oder authentifizierte rsync-Server (ideal für das Spiegeln)

27.2.3 AMANDA

AMANDA, der Advanced Maryland Automatic Network Disk Archiver, ist ein Backup-System, das es dem Administrator eines LANs erlaubt, einen einzelnen Master-Backup-Server aufzusetzen, um mehrere Hosts auf ein einzelnes Bandlaufwerk großer Kapazität zu sichern. AMANDA verwendet die nativen Dienste von dump und/oder GNU tar und kann eine große Anzahl von Workstations sichern, die unter verschiedenen Versionen von UNIX laufen. Neuere Releases von AMANDA können auch Samba dazu verwenden, Microsoft Windows Hosts zu sichern.

Mehr Informationen zu AMANDA finden Sie auf der Projekt-Seite www.amanda.org <`http://www.amanda.org/`>.

27.2.4 BOBS: Browseable Online Backup System

Browseable Online Backup System (BOBS) ist ein komplettes Online-Backup-System. Es verwendet große Platten zum Speichern von Backups und gestattet es Anwendern, die gesicherten Dateien mit einem Webbrowser zu durchsuchen. Es kann auch mit einigen speziellen Dateien umgehen, wie AppleDouble- und icon-Dateien.

Die Homepage für BOBS ist bobs.sourceforge.net <`http://bobs.sourceforge.net/`>.

Kapitel 28

HOCHVERFÜGBARKEIT

28.1 Eigenschaften und Vorzüge

Netzwerkadministratoren sind oft besorgt über die Verfügbarkeit von Datei- und Druck-Diensten. Netzwerkbenutzer sind geneigt, intolerant gegenüber den Diensten zu sein, von denen sie, was ihre Aufgabenstellungen anbelangt, abhängig sind.

Ein Schild in einem Computerraum diente dazu, das Personal an seine Verantwortung zu erinnern. Es lautete:

> Alle Menschen scheitern; sowohl im Großen wie im Kleinen scheitern wir fortwährend. Maschinen sind ebenfalls fehlerhaft. Computer sind Maschinen, die von Menschen verwaltet werden, und das Ergebnis eines Fehlers kann spektakulär sein. Ihre Verantwortung ist es, mit dem Scheitern umzugehen, es vorwegzunehmen und auszuschließen, so weit es menschlich und ökonomisch sinnvoll ist. Sind Ihre Handlungen Teil des Problems oder Teil der Lösung?

Wenn wir also mit Fehlern in geplanter und produktiver Art und Weise zu tun haben, dann müssen wir zuerst einmal das Problem verstehen. Dies ist die Zielsetzung dieses Kapitels.

In der folgenden Betrachtung sind unter anderem Informationen eingestreut, wie man Vorsorge gegen Fehler in Netzwerkinfrastrukturen trifft. Unsere Absicht ist hier keine langatmige Dissertation über die Hochverfügbarkeit selbst. Zusätzlich haben wir die bewusste Entscheidung getroffen, keine detaillierten Arbeitsbeispiele von Hochverfügbarkeitslösungen zur Verfügung zu stellen. Stattdessen zeigen wir einen Überblick über die Thematik in der Hoffnung, dass sich jemand der Herausforderung stellt, ein detailliertes Dokument zur Verfügung zu stellen, das sich ausschließlich auf die Präsentation des gegenwärtigen Wissensstandes und der Praktiken im Bereich der Hochverfügbarkeit beschränkt, soweit sie den Einsatz von Samba und anderen CIFS/SMB-Technologien betreffen.

28.2 Technische Beschreibung

Die folgende Zusammenfassung war Teil einer Präsentation von Jeremy Allison auf der SambaXP 2003-Konferenz, die im April 2003 in Göttingen abgehalten wurde. Es wurden Zusatzinformationen aus anderen Quellen hinzugefügt, aber Jeremy war es, der die folgende Struktur vorgab.

28.2.1 Das ultimative Ziel

Alle Cluster-Technologien zielen auf einen oder mehrere der folgenden Punkte ab:

- Sich die maximal erschwingliche rechnerische Power zu verschaffen
- Sich eine schnellere Programmausführung zu verschaffen
- Dienste zur Verfügung zu stellen, die nicht einfach stoppen
- Fehler zu verhindern
- Die genaue und höchsteffiziente Nutzung von Ressourcen

Ein geclusterter Dateiserver hat also idealerweise folgende Eigenschaften:

- Alle Clients können sich transparent an jeden Server verbinden.
- Ein Server kann ausfallen, und die Clients werden transparent wieder auf einen anderen Server verbunden.
- Alle Server halten denselben Satz von Dateien bereit.
- Alle Dateiänderungen sind sofort auf allen Servern zu sehen.
  - Das setzt ein verteiltes Dateisystem voraus.
- Grenzenlose Fähigkeit zu skalieren durch Hinzufügen zusätzlicher Server oder Festplatten.

28.2.2 Warum ist dies so schwer?

Kurz gesagt, das Problem ist eine Frage des *Zustands*.

- Alle TCP/IP-Verbindungen sind von Zustandsinformationen abhängig.

  Die TCP/IP-Verbindung enthält eine Paket-Sequenznummer. Diese Sequenznummer muss auf allen Maschinen in einem Cluster dynamisch aktualisiert werden, um eine nahtlose TCP-Ausfallsicherheit zu erreichen.

- CIFS/SMB (die Windows-Netzwerkprotokolle) benutzen TCP-Verbindungen.

  Dies bedeutet aus einer grundlegenden Designperspektive, dass Ausfallsicherheit nicht wirklich in Erwägung gezogen wurde.

  - Alle aktuellen SMB-Cluster sind Ausfallsicherheitslösungen, sie basieren darauf, dass die Clients sich neu verbinden. Sie stellen Server-Ausfallsicherheit zur Verfügung, aber die Clients können Informationen aufgrund eines Serverausfalls verlieren.

- Server halten Zustandsinformationen über die Client-Verbindungen fest.
  - CIFS/SMB ist in viele Zustände verwickelt.
  - Jedes Öffnen einer Datei muss mit anderen Dateiöffnungen verglichen werden, um Freigabemodi zu überprüfen.

28.2.2.1 Die Frontend-Herausforderung

Um es einem Cluster von Dateiservern zu ermöglichen, als ein einzelner Server mit einem Namen und einer IP-Adresse zu erscheinen, müssen die eingehenden TCP-Datenströme von den Arbeitsstationen durch einen virtuellen Frontend-Server verarbeitet werden. Dieser Server muss die eingehenden Pakete auf SMB-Protokoll-Layerebene de-multiplexen und dann das SMB-Paket an verschiedene Server im Cluster weiterreichen.

Einer kann dann alle IPC$-Verbindungen und RPC-Calls auf einen Server aufsplitten, um Druckaufgaben und Benutzeranfragen abzuarbeiten. RPC-Druckaufgaben werden zwischen verschiedenen IPC4-Sitzungen aufgeteilt, da es schwierig ist, diese über geclusterte Server aufzuteilen!

Konzeptionell ausgedrückt: Alle anderen Server werden nur Dateidienste zur Verfügung stellen. Sich darauf zu konzentrieren, ist ein einfacheres Problem.

28.2.2.2 De-Multiplexen von SMB-Anfragen

Das De-Multiplexen von SMB-Anfragen erfordert Wissen zu SMB-Zustandsinformationen. Alle müssen vom *virtuellen* Frontend-Server bereitgehalten werden. Dies ist ein verblüffendes und schwer zu lösendes Problem.

Windows XP und spätere Versionen von MS Windows haben die Semantik geändert, so dass Zustandsinformationen (vuid, tid, fid) für eine erfolgreiche Durchführung zueinander passen müssen. Dies macht die Dinge einfacher als zuvor und ist ein positiver Schritt vorwärts.

SMB-Anfragen werden durch vuid zu ihrem Bestimmungsserver gesendet. Es existiert zurzeit kein Code, um diese Lösung zu beeinflussen. Dieses Problem ähnelt im Grunde dem Problem, mehrere Anfragen an einen Windows 2000-Terminalserver in Samba zu bearbeiten.

Eine Möglichkeit, um damit zu beginnen ist es, den Serverpool den Clients direkt auszusetzen. Dies könnte den Schritt des De-Multiplexing überflüssig machen.

28.2.2.3 Die Herausforderung 'Verteiltes Dateisystem'

Es gibt viele verteilte Dateisysteme für UNIX und Linux.

Viele können von uns übernommen werden, um unsere Cluster abzusichern, solange wir immer die SMB-Semantik berücksichtigen (Freigabemodi, Sperren und Oplock-Themen im Speziellen). Allgemein übliche freie verteilte Dateisysteme enthalten:

- NFS
- AFS
- OpenGFS
- Lustre

Der Serverpool (Cluster) kann jedes verteilte Dateisystem-Backend nutzen, wenn die gesamte SMB-Semantik in diesem Pool durchgeführt wird.

28.2.2.4 Restriktive Zwänge in verteilten Dateisystemen

Wo ein geclusterter Server nur SMB-Dienste zur Verfügung stellt, kann das Verwalten von Oplocks direkt im Serverpool erfolgen, ohne den Zwang, diese Aufgabe an den dahinterliegenden Dateisystem-Pool weitergeben zu müssen.

Auf der anderen Seite wird es essenziell notwendig sein, dass die Implementierung Oplock-fähig ist, so dass sie mit SMB-Diensten zusammenarbeiten kann, wenn der Serverpool auch NFS oder andere Dateidienste zur Verfügung stellt. Dies ist heutzutage eine bedeutende Herausforderung. Ein Fehler dabei hat einen bemerkenswerten Perfomanceverlust zur Folge, den die Benutzer von Microsoft Windows-Clients deutlich spüren.

Zuletzt müssen alle Zustandsinformationen über den Serverpool verteilt werden.

28.2.2.5 Serverpool-Kommunikation

Die meisten Backend-Dateisysteme unterstützen die POSIX-Dateisemantik. Dies macht es schwierig, die SMB-Semantik zurück ins Dateisystem zu schieben. POSIX-Sperren haben andere Eigenschaften und eine andere Semantik als SMB-Sperren.

Alle **smbd**-Prozesse im Serverpool müssen notwendigerweise sehr schnell miteinander kommunizieren. Dadurch ist die gegenwärtig von Samba verwendete *tdb*-Dateistruktur nicht geeignet für die Nutzung über Netzwerke. Geclusterte **smbd**s müssen eine andere Struktur verwenden.

28.2.2.6 Anforderungen an die Serverpool-Kommunikation

Die Hochgeschwindigkeits-Interserverkommunikation innerhalb des Serverpools ist eine Design-Grundvoraussetzung für ein voll funktionsfähiges System. Verfügbare Möglichkeiten sind unter anderem:

- Proprietäre Shared-Memory-Bussysteme (Beispiel: Myrinet oder SCI [Scalable Coherent Interface]). Diese sind äußerst kostenintensiv.
- Gigabit-Ethernet (mittlerweile ziemlich erschwinglich)
- Raw-Ethernet-Framing (um TCP- und UDP-Overheads zu umgehen)

Wir müssen nun die Maße für Performance-Anforderungen festlegen, um dies effektiv einsetzen zu können.

28.2.2.7 Benötigte Änderungen an Samba

Samba muss entscheidend geändert werden, um mit einem Hochgeschwindigkeitsserver Inter-Connect-System zusammenzuarbeiten und transparente Ausfallsicherheits-Cluster zu erlauben.

Zu den Funktionen innerhalb von Samba, die dadurch betroffen sind, zählen:

- Die Sperren-Datenbank, Oplock-Benachrichtigungen und die Freigabemodi-Datenbank

- Die Fehlersemantik muss definiert werden. Samba verhält sich so wie Windows. Wenn Oplock-Nachrichten fehlschlagen, ist eine Anforderung zum Öffnen einer Datei erlaubt, doch dies ist in einer geclusterten Umgebung potenziell gefährlich. Wie soll also Inter-Serverpool-Fehlersemantik funktionieren, und wie soll diese implementiert werden ?

- Soll dies durch Nutzung eines Point-to-Point-Sperren-Managers implementiert werden, oder kann dies durch Multicast-Techniken erreicht werden?

28.2.3 Eine einfache Lösung

Indem man ausfallsicheren Servern erlaubt, verschiedene Funktionen innerhalb des exportierten Dateisystems zu verwalten, beseitigt man das Problem, ein verteiltes Sperrenprotokoll zu fordern.

Falls nur ein Server in einem Paar aktiv ist, wird die Forderung nach Hochgeschwindigkeits-Server-Interconnect vermieden. Dies erlaubt dann das Nutzen von vorhandenen Hochverfügbarkeitslösungen, anstatt neue erfinden zu müssen. Diese einfachere Lösung hat jedoch ihren Preis: Man muss jetzt einen wesentlich komplexeren Dateinamensbereich verwalten. Dadurch, dass es nun nicht nur ein Dateisystem gibt, müssen sich die Administratoren daran erinnern, wo all die Dienste beheimatet sind: eine Komplexität, mit der nicht einfach umzugehen ist.

Der *virtuelle Server* wird weiterhin benötigt, um Anfragen an den Backend-Server weiterzuleiten. Für die Integrität des Backend-Dateibereichs ist der Administrator verantwortlich.

28.2.4 Hochverfügbarkeits-Serverprodukte

Ausfallsichere Server müssen miteinander kommunizieren, um Ressourcenausfälle behandeln zu können. Dies ist für hochverfügbare Dienste lebensnotwendig. Der Einsatz eines dedizierten Heartbeats ist dabei eine gängige Technik, um etwas Intelligenz in den ausfallsichernden Prozess einzuführen. Dies wird oft durch einen dedizierten Link (LAN oder seriell) bewerkstelligt.

Viele Ausfallsicherungslösungen (der Red Hat Cluster Manager genauso wie Microsoft Wolfpack) können ein geteiltes SCSI von Fiberchannel Disk Storage Arrays für eine ausfallsichere Kommunikation nutzen. Informationen zu den Red Hat-Hochverfügbarkeitslösungen für Samba können Sie hier erhalten: www.redhat.com. <`http://www.redhat.com/docs/manuals/enterprise/RHEL-AS-2.1-Manual/cluster-manager/s1-service-samba.html`>

Das Linux-Hochverfügbarkeitsprojekt ist eine lesenswerte Quelle, falls Sie beabsichtigen, eine hochverfügbare Dateiserver-Lösung mit Samba aufzubauen. Bitte konsultieren Sie die Homepage www.linux-ha.org. <`http://www.linux-ha.org`>

Die Komplexität der Frontend-Server bleibt eine Herausforderung an die Hochverfügbarkeit, weil diese anständig mit Backend-Fehlern umgehen müssen, während sie zur selben Zeit den Fortlauf der Dienste für alle Netzwerkclients zur Verfügung stellen müssen.

28.2.5 MS-DFS: Der Arme-Leute-Cluster

MS-DFS Links können dazu benutzt werden, Clients zu verschiedenen Backend-Servern umzuleiten. Dies verlagert die Komplexität auf den Netzwerkclient zurück, etwas, das bereits von Microsoft vorgesehen wurde. MS-DFS erzeugt die Illusion eines einfachen und fortlaufenden Dateinamensbereichs, der sogar auf Dateiebene arbeitet.

Darüber hinaus kann, auf Kosten der Komplexität der Verwaltung, ein verteilter (Pseudo-)Cluster durch Nutzung vorhandener Samba-Funktionalität erzeugt werden.

28.2.6 Schlussfolgerungen

- Transparentes SMB-Clustering ist schwer durchzuführen!
- Client-Ausfallsicherung ist das Beste, was wir heutzutage machen können.
- Sehr viel mehr Arbeit muss erledigt werden, bevor eine praktikable und verwaltbare transparente Hochverfügbarkeits-Clusterlösung möglich sein wird.
- MS-DFS kann dazu benutzt werden, die Illusion eines einzelnen transparenten Clusters zu erzeugen.

Teil IV

Migration und Updating

Kapitel 29

UPGRADE VON SAMBA-2.X AUF SAMBA-3.0.0

Dieses Kapitel befasst sich ausschließlich mit den Unterschieden zwischen Samba-3.0.0 und Samba-2.2.8a. Es zeigt, wo in der Konfiguration Parameter geändert wurden und stellt eine einfache Anleitung für den Umstieg von 2.2.x auf 3.0.0 dar.

29.1 Kurzanleitung zur Migration

Das Standard-Verhalten von Samba-3.0.0 sollte ungefähr dasselbe sein wie das von Samba-2.2.x. Das Standard-Verhalten, wenn der neue Parameter passdb backend nicht in der Datei `smb.conf` gesetzt ist, entspricht demselben Standard-Verhalten von Samba-2.2.x mit encrypt passwords = Yes und benutzt die Datenbank `smbpasswd`.

Warum sagen wir dann, *das Verhalten sollte ungefähr dasselbe wie bei Samba-2.2.x sein?* Weil Samba-3 neue Protokolle beherrscht, z.B. die Unterstützung für Unicode, was zur Folge haben kann, dass anderer Protokoll-Code verwendet wird. Das neue Verhalten unter solchen Umständen ist nicht exakt dasselbe wie das frühere. Die gute Nachricht dabei ist, dass die Domänen- und Maschinen-SIDs beim Upgrade beibehalten werden.

Wenn das Samba-2.2.x-System ein LDAP-Backend verwendet hat und keine Zeit vorhanden ist, um die LDAP-Datenbank upzudaten, sollten Sie zumindest prüfen, dass passdb backend = ldapsam_compat in der Datei `smb.conf` gesetzt ist. Das restliche Verhalten sollte mehr oder minder das gleiche bleiben. Zu einem späteren Zeitpunkt, wenn Zeit vorhanden ist, um ein neues zu Samba-3 kompatibles LDAP-Backend zu implementieren, ist es möglich, die alte LDAP-Datenbank unter Verwendung des Befehls **pdbedit** zu migrieren (siehe Abschnitt **??**).

29.2 Neue Features in Samba-3

Die wichtigsten neuen Features sind:

1. Active Directory Support. Dieses Release kann sich einer ADS-Realm als Mitgliedsserver anschließen und Benutzer mittels LDAP/Kerberos authentifizieren.

2. Samba kann nun Unicode on-the-fly verhandeln, und es gibt intern eine viel bessere Infrastruktur für Multi-byte- und Unicode-Zeichensätze.

3. Neues Authentifizierungssystem. Das interne Authentifizierungssystem wurde fast komplett neu geschrieben. Die meisten Veränderungen sind intern, aber auch das neue Authoring-System ist sehr vielfältig konfigurierbar.

4. Neuer Befehl „*net*“. Der neue Befehl „*net*“ wurde hinzugefügt. Er ähnelt dem Windows-Befehl „*net*“. Eventuell werden einige andere Werkzeuge (wie smbpasswd) durch Sub-Befehle in „*net*“ ersetzt.

5. Samba kann nun Status32-codes von NT on-the-wire verhandeln. Dies verbessert den Umgang mit Fehlern und deren Codes deutlich.

6. Bessere Windows-200x/XP-Druck-Unterstützung, einschließlich der Bereitstellung von Drucker-Attributen im ADS.

7. Neue ladbare RPC-Module für passdb-Backends und Zeichensätze.

8. Neue standardmäßige Dual-Dämon-Unterstützung für Winbind mit besserer Performance.

9. Unterstützung für die Migration von einer Windows NT 4.0-Domäne auf eine Samba-Domäne unter Beibehaltung von Benutzer-, Gruppen- und Domänen-SIDs.

10. Unterstützung für das Herstellen von Vertrauensstellungen mit Windows NT 4.0-Domänencontrollern.

11. Initial-Unterstützung für eine verteilte Winbind-Architektur unter Verwendung eines LDAP-Verzeichnisses zur Speicherung der Zuordnungen von SIDs zu UIDs/GIDs.

12. Große Updates im Samba-Dokumentationsbaum.

13. Volle Unterstützung für Client- und Server-Signing, um für Kompatibilität mit den Standard-Sicherheitseinstellungen von Windows 2003 zu sorgen.

Und es gibt noch viele weitere Verbesserungen!

29.3 Änderungen von Konfigurationsparametern

Dieser Abschnitt enthält eine kurze Liste von Veränderungen an den Parametern in `smb.conf`, die in der Samba-Release 3.0.0 enthalten sind. Bitte konsultieren Sie die smb.conf(5)-Manpage für vollständige Beschreibungen der neuen oder geänderten Parameter.

29.3.1 Enfernte Parameter

(alphabetisch geordnet):

- admin log
- alternate permissions
- character set

- client codepage
- code page directory
- coding system
- domain admin group
- domain guest group
- force unknown acl user
- nt smb support
- post script
- printer driver
- printer driver file
- printer driver location
- status
- stip dot
- total print jobs
- use rhosts
- valid chars
- vfs options

29.3.2 Neue Parameter

(Die neuen Parameter wurden nach Funktion gruppiert):

Fernwartung

- abort shutdown script
- shutdown script

Verwaltung von Benutzer- und Gruppen-Konten:

- add group script
- add machine script
- add user to group script
- algorithmic rid base
- delete group script
- delete user from group script
- passdb backend
- set primary group script

Authentifikation:

- auth methods
- realm

Protokoll-Optionen:

- client lanman auth
- client NTLMv2 auth
- client schannel
- client signing
- client use spnego
- disable netbios
- ntlm auth
- paranoid server security
- server schannel
- server signing
- smb ports
- use spnego

Datei-Dienst:

- get quota command
- hide special files
- hide unwriteable files
- hostname lookups
- kernel change notify
- mangle prefix
- map acl inherit
- msdfs proxy
- set quota command
- use sendfile
- vfs objects

Drucken:

- max reported print jobs

Unicode und Zeichensätze:

- display charset

- dos charset
- unicode
- UNIX charset

Zuordnung von SIDs zu UIDs/GIDs:

- idmap backend
- idmap gid
- idmap uid
- winbind enable local accounts
- winbind trusted domains only
- template primary group
- enable rid algorithm

LDAP:

- ldap delete dn
- ldap group suffix
- ldap idmap suffix
- ldap machine suffix
- ldap passwd sync
- ldap user suffix

Allgemeine Konfiguration:

- preload modules
- privatedir

29.3.3 Geänderte Parameter (Änderungen im Verhalten):

- encrypt passwords (Standard-Wert: YES)
- mangling method (Standard-Wert: hash2)
- passwd chat
- passwd program
- password server
- restrict anonymous (Integer-Wert)
- security (neuer ADS-Wert)
- strict locking (Standard-Wert: YES)
- winbind cache time (erhöht auf 5 Minuten)

- winbind uid (veraltet zugunsten von idmap uid)
- winbind gid (veraltet zugunsten von idmap gid)

29.4 Neue Funktionalität

29.4.1 Datenbanken

Dieser Abschnitt enthält kurze Beschreibungen der neuen Datenbanken, die mit Samba-3 eingeführt wurden. Bitte vergessen Sie nicht, Ihre existierenden `${lock directory}/*tdb`-Dateien zu sichern, bevor Sie auf Samba-3 upgraden. Samba wird die Datenbanken upgraden, wenn sie geöffnet sind (wenn nötig), jedoch wird das Downgrade von 3.0 auf 2.2 nicht unterstützt.

Die neuen tdb-Dateien sind in Tabelle **??** beschrieben.

Tabelle 29.1. TDB-Datei-Beschreibungen

Name	Beschreibung	Backup?
account_policy	Einstellungen zu Benutzer-Richtlinien	Ja
gencache	Allgemeine Caching-DB	Nein
group_mapping	Zuordnungstabelle von Windows-Gruppen/SID zu UNIX-Gruppen	Ja
idmap	Neue Tabelle für die ID-Zuordnung von SIDs zu UNIX-UIDs/GIDs	Ja
namecache	Einträge im Namensauflösungs-Cache	Nein
printing/*.tdb	Gepufferte Ausgabe des Befehls 'lpq command', die für jeden Druckdienst angelegt wird	Nein
registry	Read-only-Samba-Registry-Gerüst, das Unterstützung für den Export verschiedener Datenbank-Tabellen via winreg-RPCs bietet	no

29.4.2 Änderungen im Verhalten

Die folgenden Themen sind bekannte Veränderungen im Verhalten zwischen Samba-2.2 und Samba-3, die manche Installationen beeinflussen können.

1. Wenn Samba-2.2 als Mitglied einer Windows-Domäne arbeitet, würde es alle Benutzer, die vom entfernten DC authentifiziert wurden, dem „*guest account*“ zuordnen, wenn keine UID durch den Aufruf **getpwnam()** erhalten werden kann. Samba-3 weist die Verbindung als „*NT_STATUS_LOGON_FAILURE*“ ab. Es gibt derzeit keine Möglichkeit, das Verhalten von Samba-2.2 wiederherzustellen.

2. Beim Hinzufügen von Maschinen zu einer Samba-2.2-Domäne wurde „*add user script*“ verwendet, um die UNIX-Identität des Maschinen-Vertrauenskontos anzulegen. Samba-3 führt „*add machine script*“ ein, das zu diesem Zweck spezifiziert werden

muss. Samba-3 wird nicht auf die Verwendung von „*add user script*“ zurückgreifen, wenn kein „*add machine script*“ vorhanden ist.

29.4.3 Passdb-Backends und Authentifikation

Es gibt einige Änderungen, an die Samba-Administratoren beim Wechsel auf Samba-3 denken sollten.

1. Verschlüsselte Passwörter sind nun standardmäßig aktiviert, um besser mit Out-of-the-box-Windows-Client-Installationen zusammenzuarbeiten. Das bedeutet, dass entweder (a) ein Samba-Konto für jeden Benutzer angelegt werden muss oder dass (b) „*encrypt passwords = no*“ explizit in `smb.conf` gesetzt sein muss.

2. Die neue Option security = ads wurde eingeführt, um die Integration einer ADS-Domäne unter Verwendung der nativen Windows-Kerberos-5- und LDAP-Protokolle zu ermöglichen.

Samba-3 beinhaltet auch die Möglichkeit, Verkettungen von Authentifikationsmethoden (auth methods) und Konten-DB-Backends (passdb backend) einzusetzen. Bitte konsultieren Sie die Manpage für `smb.conf` und Kapitel **??** „Die Account-Datenbank“ für Details. Obwohl beide Parameter auf vernünftige Standard-Werte gesetzt wurden, ist es doch wahrscheinlich, dass Sie ihre Bedeutung kennen lernen wollen, um den korrekten Betrieb von Samba zu gewährleisten.

Bestimmte Funktionen des Befehls **smbpasswd** wurden auf das neue Werkzeug **smbpasswd**, das Werkzeug **net** und das neue **pdbedit**-Utility aufgeteilt. Details dazu finden Sie in den jeweiligen Manpages.

29.4.4 LDAP

Dieser Abschnitt stellt kurz die neuen Features vor, die die Samba/LDAP-Integration betreffen.

29.4.4.1 Neues Schema

Eine neue Objektklasse (sambaSamAccount) wurde eingeführt, um die alte Klasse sambaAccount zu ersetzen. Diese Änderung hilft dabei, Attribute umzubenennen, um Kollisionen mit Attributen anderer Hersteller zu vermeiden. Es gibt ein Konverter-Skript (`examples/LDAP/convertSambaAccount`), das eine LDIF-Datei in das neue Schema konvertiert.

Beispiel:

```
$ ldapsearch .... -b "ou=people,dc=..." > old.ldif
$ convertSambaAccount <DOM SID> old.ldif new.ldif
```

Sie können <DOM SID> abfragen, indem Sie auf dem Samba PDC (als root)

```
$ net getlocalsid <DOMAINNAME>
```

ausführen.

Das alte sambaAccount-Schema kann weiterhin verwendet werden, indem man das Passdb-Backend *ldapsam_compat* spezifiziert. sambaAccount und zugehörige Attribute wurden jedoch in den „*historical*“-Abschnitt der Schema-Datei verschoben und müssen erst auskommentiert werden, um sie verwenden zu können. Die Samba-2.2-Objektklassen-Deklaration für einen sambaAccount hat sich in der samba.schema-Datei von Samba-3 nicht verändert.

Andere neue Objektklassen und deren Anwendungen beinhalten:

- sambaDomain — Domänen-Information zur Zuordnung von RIDs für Benutzer und Gruppen. Die Attribute werden im „*ldap suffix*“-Verzeichnis-Eintrag automatisch hinzugefügt, wenn ein UID/GID-Bereich für die idmap gesetzt und das „*ldapsam*“-Passdb-Backend ausgewählt wurde.
- sambaGroupMapping — Ein Objekt, das die Beziehung zwischen einer posixGroup und einer Windows-Gruppe/SID repräsentiert. Diese Einträge werden im „*ldap group suffix*“ gespeichert und mit dem Befehl „*net groupmap*“ verwaltet.
- sambaUNIXIdPool — Wird automatisch im „*ldap idmap suffix*“ angelegt und enthält die nächste verfügbare „*idmap-UID*“ und „*idmap-GID*“.
- sambaIdmapEntry — Das ist ein Objekt, das eine Zuordnung zwischen einer SID und einer UNIX-UID/GID speichert. Diese Objekte werden vom idmap_ldap-Modul je nach Bedarf angelegt.

29.4.4.2 Neues Suffix für die Suche

Die folgenden neuen smb.conf-Parameter wurden hinzugefügt, um bestimmte LDAP-Abfragen zu unterstützen, wenn *passdb backend = ldapsam://...* spezifiziert wurde.

- ldap suffix — für die Suche nach Benutzer- und Maschinen-Konten.
- ldap user suffix — für das Speichern von Benutzer-Konten.
- ldap machine suffix — für das Speichern von Maschinen-Vertrauenskonten.
- ldap group suffix — posixGroup/sambaGroupMapping-Einträge.
- ldap idmap suffix — sambaIdmapEntry-Objekte.

Wenn ein *ldap suffix* definiert ist, wird es an alle verbleibenden sub-suffix-Parameter angehängt. In diesem Fall ist die Reihenfolge der Suffixe in smb.conf wichtig. Platzieren Sie *ldap suffix* immer als ersten Eintrag in der Liste.

Wegen einer Beschränkung in Sambas Parsing von `smb.conf` sollten Sie die DNs nicht in Anführungszeichen einschließen.

29.4.4.3 Idmap-LDAP-Support

Samba-3 unterstützt ein LDAP-Backend für das idmap-Subsystem. Die folgenden Optionen informieren Samba darüber, dass die idmap-Tabelle auf dem Verzeichnis-Server „*onterose*“ in der Partition „*ou=idmap,dc=quenya,dc=org*“ gespeichert werden soll.

```
[global]
...
        idmap backend = ldap:ldap://onterose/
        ldap idmap suffix = ou=idmap,dc=quenya,dc=org
        idmap uid = 40000-50000
        idmap gid = 40000-50000
```

Bei dieser Konfiguration können Winbind-Installationen auf mehreren Servern sich einen UID/GID-Zahlenbereich teilen. Dadurch werden die Probleme bei der Zusammenarbeit mit NFS vermeiden, die es in Samba-2.2 gab.

Kapitel 30

MIGRATION VON EINEM NT4-PDC AUF EINEN SAMBA-3-PDC

Dies ist eine grobe Anleitung, um jenen zu helfen, die von NT4-basierter Domänen-Verwaltung auf Samba-3-basierte Domänen-Verwaltung migrieren wollen.

30.1 Planung und Beginn

In der IT-Welt gibt es eine Redensart, die besagt, dass alle Probleme infolge schlechter Planung entstehen. Der Folgerung daraus ist, dass nicht alle Probleme vorweggenommen und eingeplant werden können. Jedoch wird gute Planung die meisten Situationen vorwegnehmen können, die für Unterbrechungen sorgen.

Diejenigen, die von NT4-basierter Domänen-Verwaltung auf Samba-3-basierte Domänen-Verwaltung migrieren wollen, tun gut daran, einen detaillierten Migrationsplan zu entwickeln. Dazu gibt es in diesem Dokument einige Hinweise.

30.1.1 Zielsetzungen

Die hauptsächliche Zielsetzung für die meisten Organisationen wird darin bestehen, die Migration von der NT4- zur Samba-3-Domänen-Verwaltung so reibungslos wie möglich zu gestalten. Ein Problem, dem Sie in Ihrem Migrationsprozess begegnen werden, könnte sein, dass Sie das Management davon überzeugen müssen, an der neuen Umgebung festzuhalten. Viele, die OpenSource-Technologie in Unternehmen eingebracht haben, haben es erlebt, dass sie beim ersten Anzeichen von Problemen unter Druck gesetzt werden, zu Microsoft-basierten Lösungen zurückzukehren.

Bevor Sie eine Migration auf ein Samba-3-kontrolliertes Netz anstreben, sollten Sie jede Anstrengung unternehmen, um dafür Unterstützung von allen Seiten zu erhalten. Vergewissern Sie sich, dass Sie genau wissen, *warum* diese Veränderung wichtig für Ihre Organisation ist. Mögliche Motive für eine Veränderung sind:

- Sie wollen das Netzwerk-Management verbessern.

- Sie wollen eine bessere Funktionalität auf Benutzer-Ebene erreichen.
- Sie wollen die Kosten für das Betreiben des Netzwerks reduzieren.
- Sie wollen Kosten durch den Wegfall des MS-NT4-Supports reduzieren.
- Sie wollen die Auswirkungen der MS Lizenz 6 vermeiden.
- Sie wollen Ihre Abhängigkeit von Microsoft verringern.

Sorgen Sie dafür, dass jeder weiß, dass Samba-3 NICHT MS Windows NT4 ist. Samba-3 bietet eine alternative Lösung, die sich einerseits von MS Windows NT4 unterscheidet und andererseits Vorteile ihm gegenüber bietet. Erreichen Sie, dass die Verantwortlichen erkennen, dass Samba-3 viele der Features fehlen, die Microsoft als Schlüsselwerte in der Migration von MS Windows NT4 auf MS Windows 2000 und darüber hinaus beworben hat (mit oder ohne Active Directory-Dienste).

Welche Features kann Samba-3 nicht bieten?

- Active Directory Server
- Gruppen-Richtlinien-Objekte (im Active Directory)
- Maschinen-Richtlinien-Objekte
- Anmelde-Skripten im Active Directory
- Software-Anwendungs- und Zugriffskontrolle im Active Directory

Die Features, die Samba-3 anbietet und die von zwingendem Interesse für Ihre Installation sein können, sind:

- Geringere Kosten (Total Cost of Ownership, TCO)
- Globale Verfügbarkeit des Supports ohne Verpflichtungen
- Dynamische SMB-Server (mehrere SMB/CIFS-Server per UNIX/Linux-System)
- Anlegen von On-the-fly-Anmelde-Skripten
- Anlegen von On-the-fly-Richtlinien-Dateien
- Höhere Stabilität, Verlässlichkeit, Performance und Verfügbarkeit
- Administration über eine ssh-Verbindung
- Flexible Wahl der Backend-Authentifizierungstechnologie (tdbsam, ldapsam, mysql-sam)
- Mögliche Implementation einer vollen Single-Sign-On-Architektur
- Die mögliche Verteilung von Authentifizierungssystemen zur Minimierung des Bandbreiten-Bedarfs

Bedenken Sie vor der Migration eines Netzwerks von MS Windows NT4 auf Samba-3 alle notwendigen Faktoren. Die Benutzer sollten über die Änderungen, die Sie bemerken könnten, informiert werden, so dass ihnen die Umstellung willkommen und kein Hindernis, das sie von ihrer Arbeit abhält. Folgende Faktoren tragen dazu bei, eine erfolgreiche Migration zu gewährleisten:

30.1.1.1 Domänen-Entwurf

Samba-3 kann als Domänencontroller, als Backup-Domänencontroller (vielleicht am besten als sekundärer Controller bezeichnet), als Domänen-Mitgliedsserver oder als Stand-alone-Server konfiguriert werden. Der Windows-Netzwerk-Domänen-Sicherheitskontext sollte dimensioniert und geprüft werden, und zwar vor der Migration. Besondere Aufmerksamkeit sollte auf die Platzierung des PDCs und der BDCs gelegt werden. Ein Unterschied zwischen der Samba-3- und der Microsoft-Technologie ist, dass man, wenn man sich für das LDAP-Authentifizierungs-Backend entscheidet, dieselbe Datenbank für mehrere verschiedene Domänen benutzen kann. In einer komplexen Organisation kann es eine einzelne LDAP-Datenbank geben, die selbst verteilt werden kann (durch Verwendung eines Master- und mehrerer Slave-LDAP-Server) und die mehrere Domänen bedienen kann.

In Hinblick auf das Design sollte die Anzahl der Benutzer pro Server, ebenso wie die Anzahl der Server pro Domäne, unter Berücksichtigung der Server-Kapazitäten und Netzwerk-Bandbreiten festgelegt werden.

Ein physisches Netzwerk-Segment kann mehrere Domänen beinhalten. Jede Domäne kann wiederum mehrere Netzwerk-Segmente umfassen. Wenn Domänen geroutete Netzwerk-Segmente umfassen, sollten Sie die Auswirkungen auf die Performance bedenken und testen, die der Entwurf und das Design des Netzwerks haben können. Ein zentral platzierter Domänencontroller, der mehrere geroutete Netzwerk-Segmente bedienen soll, kann ernsthafte Performance-Probleme verursachen. Prüfen Sie die Antwortzeiten (ping-Zeiten) zwischen dem entfernten Segment und dem PDC. Sind diese lang ($>$ 100 ms), platzieren Sie einen BDC im entfernten Segment, um als lokaler Authentifikations- und Zugriffskontrollserver zu arbeiten.

30.1.1.2 Entwurf der Server-Freigaben und -Verzeichnisse

Es gibt einige Grundregeln des effektiven Netzwerk-Designs, die nicht ungestraft verletzt werden können. Die wichtigste und erste Regel: Einfachheit siegt. Und das in jedem gut verwalteten Netzwerk. Jeder Teil der Infrastruktur muss verwaltet werden; je komplizierter diese ist, umso größer ist die Notwendigkeit, die Systeme sicher und funktional zu halten.

Halten Sie sich vor Augen, welcher Natur die zu speichernden Daten sind. Das Layout des physischen Platten-Platzes sollte sorgfältig überlegt sein. Manche Daten müssen gesichert werden. Je einfacher das Layout ist, umso einfacher wird es sein, den Backup-Anforderungen gerecht zu werden. Legen Sie fest, welche Backup-Medien Ihren Ansprüchen gerecht werden; erwägen Sie Backups auf Band, CD-ROM (oder DVD-ROM) bzw. anderen Offline-Speicher-Medien. Planen und implementieren Sie im Hinblick auf minimalen Wartungsaufwand. Überlassen Sie nichts dem Zufall! Überlassen Sie vor allem nicht die Backups dem Zufall: Sichern, testen und überprüfen Sie jedes Backup, erstellen Sie einen Disaster-Recovery-Plan, und prüfen Sie, dass er auch funktioniert.

Benutzer sollten nach ihren Bedürfnissen, was den Datenzugriff bzw. dessen Einschränkung betrifft, gruppiert werden. Der Datei- und Verzeichniszugriff wird am besten durch Gruppen-Rechte verwaltet, und die Verwendung des „*sticky bits*“ auf gruppen-kontrollierte Verzeichnisse kann es grundlegend vermeiden, dass Benutzer von Samba-Freigaben sich über Probleme mit dem Datei-Zugriff beschweren.

Unerfahrene Netzwerk-Administratoren versuchen oft mit komplizierten Techniken Zugriffskontrollen auf Dateien, Verzeichnisse, Freigaben zu setzen und Freigaben zu definieren. Halten Sie Ihr Design und Ihre Implementation einfach, und dokumentieren Sie Ihr Design ausführlich. Lassen Sie andere Ihre Dokumentation prüfen. Schaffen Sie kein komplexes Durcheinander, das kein Nachfolgender versteht. Denken Sie daran, dass Sie Betriebsausfall und Stillstand für die Benutzer verursachen können, wenn Sie versuchen, Sicherheit durch komplexes Design und komplexe Implementation zu schaffen. Der neue Adminístrator muss nämlich erst lernen, Ihre Knoten zu entwirren. Halten Sie die Zugriffskontrollen simpel und effektiv, und stellen Sie sicher, dass die Benutzer nie durch dumme Komplexität unterbrochen werden.

30.1.1.3 Anmelde-Skripten

Anmelde-Skripten können dabei helfen, sicherzustellen, dass alle Benutzer die Freigabe- und Drucker-Verbindungen erreichen können, die sie brauchen.

Anmelde-Skripten können im Betrieb erzeugt werden, so dass alle ausgeführten Befehle spezifisch für die Rechte und Privilegien sind, die dem Benutzer erteilt wurden. Die bevorzugten Kontrollen sollten von der Gruppen-Mitgliedschaft abhängig sein, so dass die Gruppen-Information dazu benutzt werden kann, ein maßgeschneidertes Anmelde-Skript anzulegen. Dies kann durch Anwendung des Parameters root preexec in der Freigabe *NETLOGON* geschehen.

Manche Organisationen bevorzugen es, ein Werkzeug wie **kixstart** zu verwenden, um eine kontrollierte Benutzer-Umgebung zu schaffen. Jedenfalls werden Sie vielleicht mittels Google nach Programmen für Anmelde-Skripten suchen wollen. Sie sollten sich vor allem den Artikel KB189105 in der Microsoft KnowledgeBase ansehen, der beschreibt, wie man über den Logon-Skript-Vorgang Drucker ohne Benutzer-Intervention hinzufügt.

30.1.1.4 Anlegen und Migration von Profilen

Benutzer- und Gruppen-Profile können unter Verwendung der Werkzeuge migriert werden, die im Abschnitt Das Management von Desktop-Profilen beschrieben sind.

Profile können auch mit dem Samba-3-Werkzeug **profiles** verwaltet werden. Dieses Werkzeug erlaubt es, die Sicherheitsidentifier (SIDs) im MS Windows NT-Stil, die in der Profil-Datei `NTuser.DAT` gespeichert sind, auf den SID der Samba-3-Domäne zu ändern.

30.1.1.5 Benutzer- und Gruppen-Konten

Es ist möglich, alle Konten-Einstellungen von einer MS Windows NT4-Domäne auf Samba-3 zu migrieren. Bevor Sie versuchen, Benutzer- und Gruppen-Konten zu migrieren, sollten Sie UNBEDINGT in Samba die Gruppen anlegen, die in der MS Windows NT4-Domäne vorhanden sind *UND* sie auf passende UNIX/Linux-Gruppen abbilden („*mappen*“). Wenn Sie diesen einfachen Ratschlag befolgen, sollten alle Benutzer- und Gruppen-Attribute problemlos migrieren.

30.1.2 Schritte im Migrationprozess

Migrationsprozess läuft ungefähr wie folgt ab:

- Sie haben einen NT4-PDC, der die Benutzer, Gruppen, Richtlinien und Profile hat, die migriert werden sollen.
- Samba-3 ist als DC mit Netlogon-Freigabe, Profil-Freigabe und so weiter eingerichtet. Editieren Sie die Datei `smb.conf`, um Samba-3 z.B. als BDC zu konfigurieren: *`domain master = No`*.

Der Migrationsprozess der Konten

1. Legen Sie ein BDC-Konto für den Samba-Server in der alten NT4-Domäne an. Verwenden Sie dazu den NT-Server-Manager.
   (a) Samba darf nicht laufen.
2. `net rpc join -S` *`NT4PDC`* `-w` *`DOMNAME`* `-U Administrator%`*`passwd`*
3. `net rpc vampire -S` *`NT4PDC`* `-U administrator%`*`passwd`*
4. `pdbedit -L`
   (a) Achten Sie auf Folgendes: Haben die Benutzer migriert?
5. Weisen Sie nun jede der UNIX-Gruppen einer NT-Gruppe zu. (Es könnte hilfreich sein, diesen Text in ein Skript namens `initGroups.sh` zu kopieren.)

```
#!/bin/bash
#### Behalten Sie dies als Shell-Skript zur weiteren Verwendung

# Zuerst die Zuweisung der wohlbekannten globalen Domänen-Gruppen
net groupmap modify ntgroup="Domain Admins" unixgroup=root   rid=512
net groupmap modify ntgroup="Domain Users"  unixgroup=users  rid=513
net groupmap modify ntgroup="Domain Guests" unixgroup=nobody rid=514

# Nun für unsere hinzugefügten globalen Domänen-Gruppen
net groupmap add ntgroup="Designers" unixgroup=designers type=d rid=3200
net groupmap add ntgroup="Engineers" unixgroup=engineers type=d rid=3210
net groupmap add ntgroup="QA Team"   unixgroup=qateam    type=d rid=3220
```

6. `net groupmap list`
   (a) Überprüfen Sie, dass alle Gruppen erkannt werden.

Migrieren Sie alle Profile, dann migrieren Sie alle Richtlinien.

30.2 Migrationsoptionen

Organisationen, die von der MS Windows NT4-Domänen-Verwaltung auf eine Samba-basierende Lösung migrieren wollen, fallen generell in drei grundlegende Kategorien. Ta-

belle **??** zeigt die Möglichkeiten.

Tabelle 30.1. Die drei Haupttypen von Installationen

Anzahl der Benutzer	Beschreibung
< 50	Wollen eine einfache Umstellung ohne Probleme.
50 - 250	Wollen neue Funktionen, wollen manche interne Komplexität besser managen.
> 250	Die Lösung/Implementation muss gut skalieren, es gibt komplexe Anforderungen. Abteilungsübergreifender Entscheidungsprozess. Lokale Expertisen in den meisten Bereichen.

30.2.1 Den Erfolg planen

Es gibt drei grundlegende Wahlmöglichkeiten für Sites, die von MS Windows NT4 auf Samba-3 migrieren wollen:

- Einfache Konvertierung (komplettes Ersetzen)
- Erweiterte Konvertierung (könnte ein Weg der Integration sein)
- Komplettes Redesign (komplett neue Lösung)

Minimieren Sie spätere Probleme durch folgende Maßnahmen:

- Nehmen Sie sich ausreichend Zeit.
- Vermeiden Sie Panik.
- Überprüfen Sie alle Annahmen.
- Testen Sie das volle Einführungsprogramm, einschließlich der Workstations.

Tabelle **??** listet die Konvertierungsmöglichkeiten je nach angestrebtem Migrationstyp auf.

30.2.2 Wahlmöglichkeiten bei der Samba-3-Implementation

Authentifikationsdatenbank/-Backend Samba-3 kann ein externes Authentifikationsbackend verwenden:

- Winbind (externer Samba oder NT4/200x-Server)
- Externer Server, der Active Directory oder NT4 Domäne nutzt
- Kann pam_mkhomedir.so verwenden, um automatisch home-Verzeichnisse anzulegen.
- Samba-3 kann ein lokales Authentifikationsbackend verwenden: *smbpasswd, tdbsam, ldapsam, mysqlsam*

Access Control Points Samba erlaubt es, Access Control Points zu setzen:

Tabelle 30.2. Eigenschaften der Konvertierungsmöglichkeiten

Einfach	**Erweitert**	**Redesign**
Anwendung der minimalen Features des OS	Übersetzen der NT4-Features in die Features des neuen OS	Entscheide:
Bewegen aller Konten von NT4 auf Samba-3	Kopieren und verbessern	Authentifikationsregelung (Datenbank-Platzierung und -Zugriff)
Nur die notwendigsten operationalen Änderungen	Progressive Verbesserungen	Desktop-Management-Methoden
Kürzeste Migrationszeit	Auswirkungen auf Benutzer minimieren	Bessere Kontrolle über Desktops/Benutzer
Live- versus isolierter Konvertierung	Maximieren der Funktionalität	Bestimmen Sie Bedarf an: *Verwaltung, Skalierbarkeit, Sicherheit, Verfügbarkeit*
Integration von Samba-3, dann migrieren, während Benutzer aktiv sind, dann Änderung der Verwaltung (swap out)	Den Vorteils des geringeren Wartungsaufwands nutzen	

- Auf der Freigabe selbst — mittels Share ACLs
- Auf dem Dateisystem — mittels UNIX-Berechtigungen auf Dateien und Verzeichnissen

  Bemerkung: Auf diese Weise können Sie auch Posix-ACLs im Dateisystem aktivieren.
- Durch Samba-Freigaben-Parameter — . Nicht empfohlen, außer als letzte Möglichkeit.

Richtlinien (migrieren Sie sie, oder legen Sie neue an) Seien Sie äußerst vorsichtig, wenn Sie Änderungen an der Registry vornehmen, verwenden Sie das richtige Werkzeug, und denken Sie daran, dass Änderungen unter Verwendung von `NTConfig.POL`-Dateien im NT4-Stil dauerhafte Änderungen verursachen können.

- Verwendung des Group Policy Editor (NT4)
- Achten Sie auf den „*Tattoo-Effekt*“.

Benutzer- und Gruppen-Profile Diese sind plattform-spezifisch. Benutzen Sie also ein Werkzeug dieser Plattform, um von einem lokalen Profil auf ein Roaming-Profil zu wechseln. Man kann das neue Profil-Tool verwenden, um SIDs zu ändern (`NTUser.DAT`).

Anmelde-Skripten Sie müssen wissen, wie diese Skripten arbeiten.

Mapping von Benutzern und Gruppen auf UNIX/Linux Der Code zum Mapping von Benutzern und Gruppen ist neu. Viele Probleme sind aufgetaucht, als Netzwerk-Administratoren, die mit Samba-2.2.x vertraut waren, auf Samba-3 migriert haben. Lesen Sie sorgfältig die Kapitel, die das neue Verhalten des Passwort-Backends und die neue Gruppen-Mapping-Funktionalität dokumentieren.

- Die *username map*-Einrichtung könnte benötigt werden.
- Verwenden Sie **net groupmap**, um NT4-Gruppen mit UNIX-Gruppen zu verbinden.
- Verwenden Sie **pdbedit**, um die Benutzer-Konfigurationen zu setzen und zu ändern.

  Beim Migrieren auf LDAP kann es einfacher sein, die anfängliche LDAP-Datenbank als LDIF-Datei auszugeben, zu editieren und wieder in LDAP einzulesen.

OS-spezifische Skripten/Programme könnten benötigt werden Jedes Betriebssystem hat seine Besonderheiten. Diese sind das Ergebnis von Entscheidungen, die auf den Erfahrungen des Designers beruhen. Sie können Nebeneffekte haben, die nicht beabsichtigt waren. Zu den Einschränkungen, die den Windows-Netzwerk-Administrator betreffen können, zählen:

- Hinzufügen/Löschen von Benutzern: Beachten Sie die Beschränkungen des Betriebssystems in Hinblick auf Länge des Benutzernamens (Linux 8 Zeichen, NT4 bis zu 254 Zeichen).
- Hinzufügen/Löschen von Maschinen: Betrifft nur Domänen-Mitglieder (Bemerkung: Maschinen-Namen können auf 16 Zeichen beschränkt sein).
- Verwendung von **net groupmap**, um NT4-Gruppen mit UNIX-Gruppen zu verbinden.
- Hinzufügen/Löschen von Gruppen: Beachten Sie Beschränkungen des Betriebssystems bei Länge und Format. Das Limit in Linux sind 16 Zeichen ohne Leerzeichen und Großbuchstaben (**groupadd**).

Migrationswerkzeuge Domänenverwaltung (im NT4-Stil) Profile, Richtlinien, ACLs, Sicherheit

- Samba: **net, rpcclient, smbpasswd, pdbedit, profiles**
- Windows: **NT4 Domain User Manager, Server Manager (NEXUS)**

Kapitel 31

SWAT — DAS SAMBA-ADMINISTRATIONS-WERKZEUG

Es gibt viele und verschiedene Meinungen über den Nutzen von SWAT. Gleichgültig wie viel Mühe man sich gibt, ein perfektes Konfigurationswerkzeug zu erstellen; die Benutzung ist eine Frage des persönlichen Geschmacks. SWAT ist ein Werkzeug, das eine web-basierte Konfiguration von Samba ermöglicht. Es beinhaltet einen Wizard zur schnellen Konfiguration von Samba, besitzt eine kontextabhängige Hilfe für jeden Parameter der `smb.conf`, überwacht den aktuellen Zustand der Verbindung und erlaubt eine netzwerkweite Passwortverwaltung für MS Windows.

31.1 Eigenschaften und Vorzüge

SWAT ist Teil der Samba-Suite. Das Hauptprogramm heißt **swat** und wird über **xinetd** gestartet (siehe Abschnitt **??** für Einzelheiten).

SWAT verwendet Samba-eigene Komponenten, um die von der jeweiligen Samba-Version unterstützten Parameter zu lokalisieren. Anders als externe Werkzeuge und Hilfsmittel bleibt SWAT bei Parameteränderungen auf dem aktuellsten Stand. SWAT eine bietet kontextabhängige Hilfe fuer jeden Konfigurationsparameter direkt aus Manpage-Einträgen heraus.

Manche Netzwerkadministratoren schreiben Dokumentationen in Form von Kommentaren innerhalb von Konfigurationsdateien. Für diese wird SWAT ein eher unbeliebtes Werkzeug sein. SWAT speichert die Konfigurationsdatei in keiner Mischform, sondern speichert ausschließlich Parameterwerte. Wenn SWAT also die `smb.conf` schreibt, schreibt es nur jene Parameter, die von den Standardwerten abweichen. Das bedeutet, dass Kommentare und nicht unterstützte Parameter nicht mehr in der `smb.conf` erscheinen werden. Dazu werden die Parameter in eine interne Reihenfolge geschrieben.

ANMERKUNG

Eine Warnung, bevor Sie SWAT benutzen: SWAT ersetzt eine bereits im System vorhandene `smb.conf` durch eine von SWAT optimierte Version, aus der alle vorher eingefügten Kommentare und Nicht-Standardwerte entfernt worden sind.

31.2 Grundlagen und technische Hilfen

Dieser Abschnitt erklärt, wie man SWAT aktiviert, wie man es sicherer macht und wie man Probleme bei der Internationalisierung löst.

31.2.1 Überprüfen der SWAT-Installation

Bevor Sie beginnen, einen Rechner für SWAT zu konfigurieren, sollten Sie überprüfen, ob es überhaupt installiert ist. Dies mag einigen trivial erscheinen, dennoch installieren einige Distributionen SWAT nicht standardmäßig, obwohl es auf den Medien des Distributors vorhanden ist.

Wenn Sie sich sicher sind, dass SWAT installiert ist, müssen Sie überprüfen, dass die Installation das Binary **swat** sowie alle unterstützenden Text- und Webseiten enthält. Bei einer Reihe von Linux-Distributionen fehlten diese vollständig, obwohl das **swat**-Binary installiert war.

Wenn Sie sich davon überzeugt haben, dass wirklich alles installiert ist, müssen Sie prüfen, dass SWAT in der Kontrolldatei von inetd oder xinetd aktiviert ist, je nachdem, welcher von beiden Daemons vom Betriebssystem verwendet wird.

31.2.1.1 Lokalisieren der Datei swat

Um sicherzustellen, dass SWAT installiert ist, lokalisiert man das Binary **swat** im System. Es könnte in folgenden Verzeichnissen liegen:

- `/usr/local/samba/bin` — der standardmäßige swat Pfad.
- `/usr/sbin` — der Standardort vieler Linux-Systeme.
- `/opt/samba/bin`

Der tatsächliche Speicherort hängt von der Wahl des Bestriebssystemdistributors ab oder davon, welchen Installationspfad der Administrator gewählt hat.

Es gibt eine Anzahl verschiedener Methoden, um den Ort der Installation des **swat**-Binarys festzustellen. Die folgenden Methoden können hilfreich sein:

Wenn **swat** sich im aktuellen Suchpfad des Betriebssystems befindet, ist es einfach zu finden. Man kann sich die Kommandoparameter von **swat** wie folgt anzeigen lassen:

```
frodo:~ # swat -?
Usage: swat [OPTION...]
```

```
  -a, --disable-authentication         Authentifizierung abschalten (demo mode)

Help options:
  -?, --help                           Zeigt diese Hilfe an
  --usage                              Zeigt eine kurze Benutzerhilfe an

Common samba options:
  -d, --debuglevel=DEBUGLEVEL          Setzt den Debug-Level
  -s, --configfile=CONFIGFILE          Benutzt eine alternative Konfigurationsdatei
  -l, --log-basename=LOGFILEBASE       Basisname für Log/Debug-Dateien
  -V, --version                        Gibt die Version aus
```

31.2.1.2 Lokalisieren der Hilfedateien zu SWAT

Nachdem Sie herausgefunden haben, dass **swat** im Suchpfad ist, ist es einfach, es im System zu identifizieren. Hier ist eine andere einfache Methode, dies zu bewerkstelligen:

```
frodo:~ # whereis swat
swat: /usr/sbin/swat /usr/share/man/man8/swat.8.gz
```

Wenn dieser Versuch, das **swat**-Binary zu finden, misslingt, ist ein weiterer Versuch notwendig:

```
frodo:/ # find / -name swat -print
/etc/xinetd.d/swat
/usr/sbin/swat
/usr/share/samba/swat
frodo:/ #
```

Die Ausgabe zeigt, dass eine Kontrolldatei für **xinetd** auf der Maschine vorhanden ist. Der Ort der SWAT-Binary-Datei ist `/usr/sbin/swat`, und die Hilfedateien befinden sich im Verzeichnis `/usr/share/samba/swat`.

Im Folgenden muss überprüft werden, wo **swat** seine Hilfsdateien vermutet. Dies kann wie folgt geschehen:

```
frodo:/ # strings /usr/sbin/swat | grep "/swat"
/swat/
...
/usr/share/samba/swat
frodo:/ #
```

Der Eintrag `/usr/share/samba/swat/` ist der Ort, an dem sich die von SWAT benötigten Dateien befinden. Um sicherzustellen, dass alle Dateien in diesem Verzeichnis vorhanden

sind, gibt man Folgendes ein:

```
jht@frodo:/> find /usr/share/samba/swat -print
/usr/share/samba/swat
/usr/share/samba/swat/help
/usr/share/samba/swat/lang
/usr/share/samba/swat/lang/ja
/usr/share/samba/swat/lang/ja/help
/usr/share/samba/swat/lang/ja/help/welcome.html
/usr/share/samba/swat/lang/ja/images
/usr/share/samba/swat/lang/ja/images/home.gif
...
/usr/share/samba/swat/lang/ja/include
/usr/share/samba/swat/lang/ja/include/header.nocss.html
...
/usr/share/samba/swat/lang/tr
/usr/share/samba/swat/lang/tr/help
/usr/share/samba/swat/lang/tr/help/welcome.html
/usr/share/samba/swat/lang/tr/images
/usr/share/samba/swat/lang/tr/images/home.gif
...
/usr/share/samba/swat/lang/tr/include
/usr/share/samba/swat/lang/tr/include/header.html
/usr/share/samba/swat/using_samba
...
/usr/share/samba/swat/images
/usr/share/samba/swat/images/home.gif
...
/usr/share/samba/swat/include
/usr/share/samba/swat/include/footer.html
/usr/share/samba/swat/include/header.html
jht@frodo:/>
```

Wenn die oben aufgelisteten Dateien nicht vorhanden sind, müssen Sie diese installieren, da sich SWAT sonst nicht verwenden lässt.

31.2.2 SWAT aktivieren

SWAT sollte installiert werden, um es über den Netzwerk-Daemon starten zu können. Je nach UNIX/Linux-System ist dies entweder **inetd** oder **xinetd**.

Die Vorgehensweise und der Ort variieren hierbei je nach verwendetem Betriebssystem. Die Kontrolldatei (oder -dateien) finden Sie im Allgemeinen unter `/etc/inetd.conf` oder (für xinetd) im Verzeichnis `/etc/[x]inet[d].d`.

Der Eintrag für den älteren Typ der Kontrolldatei kann sein:

```
   # swat is the Samba Web Administration Tool
   swat stream tcp nowait.400 root /usr/sbin/swat swat
```

Ein Eintrag für die neuere Variante der Kontrolldatei in xinetd könnte so aussehen:

```
# default: off
# description: SWAT is the Samba Web Admin Tool. Use swat \
#              to configure your Samba server. To use SWAT, \
#              connect to port 901 with your favorite web browser.
service swat
{
   port    = 901
   socket_type     = stream
   wait    = no
   only_from = localhost
   user    = root
   server  = /usr/sbin/swat
   log_on_failure  += USERID
   disable = yes
}
```

Beide der oben angegebenen Beispiele setzen voraus, dass **swat** im `/usr/sbin` Verzeichnis liegt. Zusätzlich benötigt SWAT ein Verzeichnis, in dem es sowohl die Hilfedateien als auch die Kontrollinformationen findet. Der Standardpfad für dieses Verzeichnis ist auf den meisten Linux-Systemen `/usr/share/samba/swat`. Der Pfad für die Samba-Standards ist `/usr/local/samba/swat`.

Bei einem Zugriff auf SWAT wird nach einer Anmeldung gefragt. Wenn man sich in SWAT als Nicht-Root-Benutzer anmeldet, ist man ausschließlich dazu berechtigt, einige bestimmte Konfigurationsoptionen nur zu lesen sowie auf die Passwortverwaltung zuzugreifen. Die für Nicht-Root-Benutzer angezeigten Buttons sind: **HOME**, **STATUS**, **VIEW** und **PASSWORD**. Die einzige Seite, die Änderungen erlaubt, ist **PASSWORD**.

Meldet man sich als Benutzer *root* an, erhält man volle Kontrolle über sämtliche Funktionen in SWAT. Die angezeigten Buttons sind: **HOME**, **GLOBALS**, **SHARES**, **PRINTERS**, **WIZARD**, **STATUS**, **VIEW** und **PASSWORD**.

31.2.3 Absichern von SWAT mit SSL

Viele Leute haben gefragt, wie man SWAT mit SSL aufsetzt, um so eine sichere Fernadministration zu erlauben. Hier ist eine funktionierende Methode, die von Markus Krieger zur Verfügung gestellt worden ist.

Nehmen Sie folgende Modifikationen bei der SWAT-Installation vor:

1. Installieren Sie OpenSSL.
2. Generieren Sie ein Zertifikat und einen privaten Schlüssel.

```
root# /usr/bin/openssl req -new -x509 -days 365 -nodes -config \
   /usr/share/doc/packages/stunnel/stunnel.cnf \
   -out /etc/stunnel/stunnel.pem -keyout /etc/stunnel/stunnel.pem
```

3. Entfernen Sie den swat-Eintrag aus [x]inetd.
4. Führen Sie **stunnel** aus.

```
root# stunnel -p /etc/stunnel/stunnel.pem -d 901 \
    -l /usr/local/samba/bin/swat swat
```

Danach verbinden Sie sich einfach mit SWAT über die URL <`https://myhost:901`>, akzeptieren das Zertifikat, und die SSL-Verbindung steht.

31.2.4 Die Mehrsprachenunterstützung von SWAT aktivieren

SWAT kann so konfiguriert werden, dass es seine Nachrichten in der Sprache anzeigt, die in Ihrem Webbrowser eingestellt ist. Diese Anweisung wird SWAT im Accept-Language-Header der HTTP-Anfrage übergeben.

Um dieses Feature zu aktivieren, tun Sie Folgendes:

- Installieren Sie die passenden **msg**-Dateien aus dem Samba-`source/po`-Verzeichnis nach $LIBDIR.
- Setzen Sie den korrekten Wert für display charset.
- Stellen Sie die Sprache im Browser ein.

Der Name der msg-Datei entspricht der Sprach-ID des Browsers, zum Beispiel en für „*English*“, de für „*Deutsch*“, ja für „*Japanisch*“ oder fr für „*Französisch*“.

Wenn Ihnen einige der Nachrichten nicht gefallen oder keine **msg**- Dateien für Ihre eigene oder Ihre präferierte Sprache vorhanden sind, können Sie einfach die **en.msg**-Dateien in das Verzeichnis für „*Meine Sprache ID.msg*“ kopieren und passende Nachrichten zu jedem „*msgstr*“ eintragen. Zum Beispiel trägt man für `it.msg` (die **msg**-Datei für Italienisch) Folgendes ein:

```
msgid "Set Default"
msgstr "Imposta Default"
```

usw. Wenn Sie einen Fehler finden oder eine neue **msg**-Datei erstellt haben, mailen Sie (diese) bitte, damit wir sie für das nächste Release von Samba bereitstellen können.

Zusätzlich sei erwähnt, dass die Ausgabe von SWAT durcheinander geraten kann, wenn dieses Feature aktiviert wird, aber display charset nicht mit der im Browser eingestellten

Sprache übereinstimmt. In einer zukünftigen Samba-Version wird SWAT immer UTF-8-kodierte Nachrichten anzeigen. Es wird dann nicht mehr nötig sein, den `smb.conf`-Parameter für die Sprache zu setzen.

31.3 Übersicht und ein Schnelldurchlauf

SWAT ist ein Werkzeug, das von vielen genutzt wird, um Samba zu konfigurieren. Sie können damit aber auch einfach auf die nützlichen Links zu wichtigem Referenzmaterial (z.B. auf den Inhalt dieser Dokumentation) oder auf andere Dokumente zugreifen, die Ihnen dabei helfen können, Probleme mit dem Windows-Netzwerk zu lösen.

31.3.1 Die Homepage von SWAT

Die SWAT-Titelseite bietet Zugriff auf die aktuellste Samba-Dokumentation. Von dieser Seite aus kann auf die Manual-Pages jeder Samba-Komponente zugegriffen werden, auf die Samba HOWTO-Sammlung (dieses Buch) und auf das Buch „*Samba*“ von O'Reilly.

Administratoren, die ihre Samba-Konfiguration überprüfen möchten, finden nützliche Informationen in den Manpages der einzelnen Diagnose-Werkzeuge, die auch auf der SWAT-Homepage im Internet verfügbar sind. Ein nicht erwähntes, aber teils nützliches Diagnose-Werkzeug finden Sie unter **ethereal**. <`http://www.ethereal.com/`>

> WARNUNG
>
> SWAT kann so konfiguriert werden, dass es in einem *Demo*-Modus läuft. Dieser Modus wird nicht empfohlen, da er SWAT ohne Authentifizierung, aber mit sämtlichen administrativen Möglichkeiten ausführt. Er erlaubt Änderungen an der `smb.conf` wie auch alle anderen Tätigkeiten mit root-Rechten. Die Option, die dies erlaubt, ist das `-a` Flag für swat. *Verwenden Sie diesen Modus nicht in einer Produktionsumgebung!*

31.3.2 Globale Einstellungen

Der **GLOBALS**-Button öffnet die Seite, auf der es möglich ist, die globalen Parameter in der `smb.conf` zu konfigurieren. Es gibt zwei Arten, wie diese Parameter angezeigt werden:

- **Basic** — Zeigt allgemeine Konfigurationsoptionen an.
- **Advanced** — Zeigt Konfigurationsoptionen an, die in komplexeren Umgebungen gebraucht werden.

Um die Optionen im erweiterten Modus zu editieren, klicken Sie auf **Advanced**, im anderen Fall auf **Basic**. Sie können auch zuerst auf den Radio-Button klicken und dann auf den **Commit Changes**-Button.

Nachdem Sie Änderungen an Konfigurationsparametern vorgenommen haben, sollten Sie noch einmal prüfen, dass Sie auf den **Commit Changes**-Button gedrückt haben, bevor Sie die Seite verlassen, da sonst alle Änderungen verloren gehen.

ANMERKUNG

SWAT besitzt eine kontextabhängige Hilfe. Um herauszufinden, wofür jeder Parameter steht und welchen Zweck er erfüllt, klicken Sie auf den Link **Help** links neben dem Konfigurationsparameter.

31.3.3 Einstellungen zur Freigabe (Share)

Um eine bereits konfigurierte Freigabe zu bearbeiten, klicken Sie auf das Pulldown-Menü zwischen **Choose Share** und **Delete Share** und wählen die Freigabe aus, mit der man arbeiten will. Um die Einstellungen zu editieren, klicken Sie auf den Button **Choose Share**. Um die Freigabe zu löschen, klicken Sie auf den Button **Delete Share**.

Um eine neue Freigabe zu erzeugen, geben Sie den Namen der Freigabe in ein Textfeld ein, das sich neben dem mit **Create Share** beschrifteten Button befindet. Die Freigabe erzeugt man schließlich mit **Create Share**.

31.3.4 Druckereinstellungen

Einen bereits eingerichteten Drucker bearbeiten Sie mit dem Pulldown-Menü zwischen **Choose Printer** und **Delete Printer**. Wählen Sie hier den Drucker aus, den Sie bearbeiten wollen. Um die Einstellungen zu bearbeiten, benutzen Sie den Button **Choose Printer**; um den Drucker aus der Liste zu löschen, klicken Sie auf **Delete Printer**.

Einen neuen Drucker legen Sie in dem Textfeld neben dem Button **Create Printer** an, indem Sie den Namen des freizugebenden Druckers eingeben. Sie geben ihn schließlich frei, indem Sie auf **Create Printer** klicken.

31.3.5 Der SWAT-Wizard

Der Zweck des SWAT-Wizards ist es, dem sachkundigen MS-Netzwerkadministrator die Konfiguration von Samba so einfach wie möglich zu machen.

Die Wizard-Seite bietet ein Werkzeug, um die Datei `smb.conf` in einem optimierten Format zurückzuschreiben. Genau dies geschieht auch, wenn Sie auf den Button **Commit** klicken. Der Unterschied zwischen dem **Rewrite**-Button und dem **Commit**-Button ist, dass **Rewrite** alle Änderungen ignoriert und **Commit** sämtliche vorgenommenen Änderungen umsetzt.

Der **Edit**-Button erlaubt das Editieren der Minimaloptionen, die notwendig sind, um einen funktionsfähigen Samba-Server zu konfigurieren.

Schließlich gibt es noch eine begrenzte Anzahl von Optionen, die bestimmen, wofür der Samba-Server konfiguriert werden soll: ob er als WINS-Server dienen soll, als WINS-Client am Netz teilnimmt oder ob er ohne WINS-Unterstützung arbeiten soll. Mit einem Klick können Sie auswählen, ob Sie die Heimatverzeichnisse der Benutzer freigeben wollen.

31.3.6 Die Status-Seite

Die Status-Seite erfüllt nur einen geringen Nutzen. Sie erlaubt die Überwachung der Samba-Daemons, wobei die Hauptdaemons, aus denen der Samba-Server besteht, smbd, nmbd und winbindd sind.

Die Daemons können individuell oder als eine zusammenhängende Gruppe überwacht werden. Zusätzlich kann man eine automatische Aktualisierung der Seite einstellen. Wenn MS Windows-Clients mit Samba interagieren, werden kontinuierlich neue smbd-Prozesse eingepflegt. Mit minimalem Aufwand können Sie über die automatische Aktualisierung sich ändernde Zustände verfolgen.

Zuletzt können Sie die Status-Seite auch dazu benutzen, bestimmte smbd-Clientverbindungen zu unterbrechen, um Dateien freizugeben, die u.U. gesperrt sind.

31.3.7 Die Übersichtsseite

Sie ermöglicht es dem Administrator, sich die optimierte `smb.conf`-Datei anzusehen, und erlaubt es den Masochisten unter uns, alle möglichen globalen Konfigurationsparameter und ihre Einstellungen anzuschauen.

31.3.8 Die Seite zur Passwortänderung

Die Seite zur Passwortänderung ist ein sehr beliebtes Werkzeug, das das Erstellen, Löschen, De- und Reaktivieren von MS-Windows-Benutzern auf der lokalen Maschine erlaubt. Alternativ kann man es zur Änderung von lokalen Passwörtern verwenden.

Wenn der Benutzer als Nicht-Root-Benutzer angemeldet ist, muss er bei Änderungen von Passwörtern das alte und zweimal das neue Passwort eingeben. Ist er als *root* angemeldet, wird nur das neue Passwort benötigt.

Das Werkzeug wird auch oft dazu genutzt, Benutzerpasswörter über eine Reihe von MS Windows-Servern hinweg zu ändern.

31.4 Fehlerhafte Ausgaben der Übersichtsseite von SWAT

Wenn sich die Parameter *`display charset`* und *`dos charset`* voneinander unterscheiden, wird die Übersichtsseite fehlerhaft angezeigt. Der Parameter *`display charset`* muss dieselbe Kodierung wie die msg-Datei besitzen. Falls Sie eine japanische Schrift brauchen, müssen Sie *`display charset`* auf *`CP932`* setzen.

Das Problem entsteht auf, wenn Sie *`unix charset = EUCJP-MS`* setzen.

Teil V

Troubleshooting

Kapitel 32

DIE SAMBA-CHECKLISTE

32.1 Einleitung

Dieses Dokument beschreibt eine Reihe von Tests zur Überprüfung Ihres Samba-Servers. Wenn bei den Tests Probleme festgestellt werden, bietet es ferner Informationen über die möglichen Fehlerursachen. Wurden alle Tests fehlerfrei durchgeführt, sollte alles einwandfrei funktionieren.

Sie sollten alle Tests in der genannten Reihenfolge durchführen. Wir haben sorgfältig versucht, die Reihenfolge so auszuwählen, dass nachfolgende Tests auf erfolgreich durchgeführte frühere Tests aufbauen. Auch nachdem Sie einen Fehler behoben haben, sollten Sie immer alle Tests komplett durchführen.

Wenn Sie eine E-Mail mit dem Inhalt „*Es funktioniert nicht*“ an eine der Samba-Mailinglisten schicken, ohne diese Tests durchgeführt zu haben, so wundern Sie sich bitte nicht, wenn Ihre E-Mail ingoriert wird.

32.2 Vorbemerkung

In allen Tests wird davon ausgegangen, dass Sie einen Samba-Server BIGSERVER und einen PC ACLIENT haben, die sich in der Arbeitsgruppe TESTGROUP befinden.

Das Vorgehen ist für andere Typen von Clients ähnlich.

Des Weiteren wird angenommen, dass Sie den Namen einer verfügbaren Freigabe in Ihrer `smb.conf` kennen. Ich werde hier die Freigabe mit dem Namen *tmp* verwenden. Sie können solch eine Freigabe durch folgende Zeilen erstellen (siehe Beispiel **??**).

Beispiel 32.2.1. smb.conf mit [tmp]-Freigabe

```
[tmp]
        comment = temporary files
        path = /tmp
        read only = yes
```

ANMERKUNG

Diese Tests setzen Samba in der Version 3.0.0 oder später voraus. Einige der genannten Befehle sind in früheren Samba-Versionen nicht enthalten.

Bitte schenken Sie den gemeldeten Fehlermeldungen Ihre Aufmerksamkeit. Sollten Sie eine Fehlermeldung erhalten, dass Ihr Server „*unfriendly*“ wäre, überprüfen Sie bitte, ob Ihre IP-Namensauflösung korrekt eingestellt ist. Stellen Sie sicher, dass in der Datei `/etc/resolv.conf` ein korrekter Nameserver eingetragen wurde.

Sollten Sie keinen DNS-Server einsetzen, überprüfen Sie, ob Ihre `smb.conf` die Zeile **dns proxy = no** enthält. Der beste Weg, das zu überprüfen, ist der Befehl **testparm smb.conf**.

Es ist hilfreich, während der Tests die Log-Dateien in einem separaten Konsolenfenster (mit „*Ctrl-Alt-F1*“ bis „*Ctrl-Alt-F6*“ oder mehrere Fenster in X) mit Hilfe von **tail -F log_file_name** zu überwachen. Die wichtigen Log-Dateien finden Sie (in der Default-Installation) unter `/usr/local/samba/var`. Sie können hier des Weiteren die Verbindunglogs von Computern finden - oder evtl. auch in `/var/log/samba`, je nachdem, wie Sie es in `smb.conf` angegeben haben.

Sollten Sie während der Tests Änderungen an der `smb.conf` durchführen, vergessen Sie bitte nicht, smbd und nmbd neu zu starten.

32.3 Die Tests

Diagnose Ihres Samba-Servers

1. Rufen Sie im Verzeichnis Ihrer `smb.conf` den Befehl **testparm smb.conf** auf. Werden Fehler angezeigt, ist Ihre `smb.conf` nicht in Ordnung.

   ANMERKUNG

   Ihre `smb.conf` sollte in `/etc/samba` oder in `/usr/local/samba/lib` zu finden sein.

2. Führen Sie auf Ihrem PC den Befehl **ping BIGSERVER** und auf Ihrem Unix-Server den Befehl **ping ACLIENT** aus. Erhalten Sie keine gültige Antwort, so ist TCP/IP nicht korrekt eingerichtet. Sie müssen an Ihrem PC eine „*DOS-Eingabeaufforderung*“ öffnen, um den Befehl ping auszuführen. Erhalten Sie eine Meldung in der Art von „*host not found*“, dann ist Ihre DNS-Konfiguration oder die Datei `/etc/hosts` nicht in Ordnung. Es ist möglich, Samba ohne DNS-Einträge für den Server oder die Clients zu betreiben, aber es wird für die weiteren Tests davon ausgegangen, dass diese Einträge

korrekt sind. Eine weitere Möglichkeit, warum ein ping nicht funktioniert, ist eine vorhandene Firewall. Sie müssen die Regeln der Firewall dahingehend anpassen, dass Sie die Workstation evtl. von einem anderen Subnetz aus zugreifen lassen können. Unter Linux können Sie dies mit den Firewall-Programmen **ipchains** oder **iptables** durchführen.

ANMERKUNG

Moderne Linux-Distributionen installieren per Default ipchains/iptables. Das ist ein gängiges Problem und wird häufig übersehen.

Möchten Sie die Firewall-Regeln des Testsystems überprüfen, rufen Sie einfach **iptables -L -v** oder bei *ipchains*-basierenden Firewalls **ipchains -L -v** auf. Das Folgende ist eine Beispielausgabe eines System mit einer externen Ethernet-Schnittstelle (eth1), an der Samba nicht aktiv ist, und einer internen (privates Netzwerk) Ethernet-Schnittstelle (eth0), an der Samba aktiv ist.

```
frodo:~ # iptables -L -v
Chain INPUT (policy DROP 98496 packets, 12M bytes)
 pkts bytes target     prot opt in     out     source     destination
 187K  109M ACCEPT     all  --  lo     any     anywhere   anywhere
 892K  125M ACCEPT     all  --  eth0   any     anywhere   anywhere
1399K 1380M ACCEPT     all  --  eth1   any     anywhere   anywhere  \
               state RELATED,ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source     destination
 978K 1177M ACCEPT     all  --  eth1   eth0    anywhere   anywhere \
               state RELATED,ESTABLISHED
 658K   40M ACCEPT     all  --  eth0   eth1    anywhere   anywhere
    0     0 LOG        all  --  any    any     anywhere   anywhere \
               LOG level warning

Chain OUTPUT (policy ACCEPT 2875K packets, 1508M bytes)
 pkts bytes target     prot opt in     out     source     destination

Chain reject_func (0 references)
 pkts bytes target     prot opt in     out     source     destinat
```

3. Führen Sie auf Ihrer Unix-Maschine den Befehl **smbclient -L BIGSERVER** aus. Sie sollten eine Liste der verfügbaren Freigaben erhalten. Sollten Sie die Meldung „*Bad password*“ erhalten, so dürfte es sich um einen falschen Eintrag bei *hosts allow*, *hosts deny* oder *valid users* in Ihrer `smb.conf` handeln, oder der guest account ist nicht gültig. Überprüfen Sie mit testparm Ihren guest account, und entfernen

Sie testweise alle *hosts allow*-, *hosts deny*-, *valid users*- oder *invalid users*-Einträge. Erhalten Sie eine Meldung „*connection refused*“, dann läuft der **smbd**-Prozess nicht. Haben Sie diesen in `inetd.conf` eingetragen, so stimmt evtl. dieser Eintrag nicht. Haben Sie diesen als Daemon installiert, überprüfen Sie mit **netstat -a**, ob dieser gestartet ist und ob der netbios-ssn-Port den Status LISTEN hat.

ANMERKUNG

Einige UNIX/Linux-Systeme verwenden **xinetd** anstelle von **inetd**. Lesen Sie in Ihrer System-Dokumentation die Infos über die entsprechende Implementation Ihres Netzwerk-Super-Daemons nach.

Erhalten Sie die Meldung „*session request failed*“, dann lehnt der Server eine Verbindung ab. Lautet die Information „*Your server software is being unfriendly*“, dann könnten Sie wahrscheinlich einen falschen Startparameter für smbd angegeben haben oder es besteht ein ähnliches grundsätzliches Problem beim Starten von smbd. Testen Sie mit testparm Ihre Config-Datei (`smb.conf`) auf Syntax-Fehler und darauf, dass die diversen Log- und Lock-Verzeichnisse von Samba vorhanden sind. Es gibt eine Menge von Gründen dafür, dass smbd eine Verbindung ablehnt oder verweigert. Die häufigsten Gründe dürften an folgenden Einträgen in der `smb.conf` liegen (siehe Beispiel **??**).

Beispiel 32.3.1. Konfiguration für erlaubte Verbindungen eines bestimmten Subnetzes

```
[globals]
...
        hosts deny = ALL
        hosts allow = xxx.xxx.xxx.xxx/yy
        interfaces = eth0
        bind interfaces only = Yes
...
```

Im obigen Beispiel werden keinerlei Verbindungsanforderungen erlaubt, da diese durch die Adresse des Loopback-Devices 127.0.0.1 ersetzt werden. Um das Problem zu lösen, ändern Sie die folgenden Zeilen in Beispiel **??**

Eine weitere oft vorkommende Ursache dieser zwei Fehlermeldungen ist ein bereits laufender an Port `139`, etwa ein durch inetd gestarteter Samba-Daemon smbd oder etwas Vergleichbares wie Digital's Pathworks. Überprüfen Sie daher vor dem Start von smbd als Daemon Ihre `inetd.conf`, um eine Menge Frustration zu vermeiden. Eine weitere mögliche Ursache für ein Scheitern dieses Tests besteht darin, dass die Subnetz-Maske und/oder die Broadcast-Adresse nicht korrekt ist. Bitte überprüfen Sie daher die korrekte Broadcast/Subnetz- Maske Ihres Netzwerkinterfaces und stellen Sie sicher, dass Samba diese Einstellungen in der `log.nmbd`-Datei bestätigt.

Beispiel 32.3.2. Konfiguration für erlaubte Verbindungen eines bestimmten Subnetzes und von localhost

```
[globals]
...
        hosts deny = ALL
        hosts allow = xxx.xxx.xxx.xxx/yy 127.
        interfaces = eth0 lo
...
```

4. Führen Sie den Befehl **nmblookup -B BIGSERVER __SAMBA__** aus. Sie sollten die IP-Adresse Ihres Samba-Servers gemeldet bekommen. Wenn nicht, ist nmbd nicht korrekt installiert. Überprüfen Sie Ihre `inetd.conf`, wenn er durch inetd gestartet wird, oder dass er als Daemon läuft und am UDP-Port 137 lauscht. Ein häufiges Problem sind inetd-Implementationen, die nicht mehrere Parameter auf der Kommandozeile verarbeiten können. Ist das bei Ihnen der Fall, erstellen Sie ein einzeiliges Skript mit den richtigen Parametern, und starten Sie dieses durch inetd.

5. Starten Sie den Befehl **nmblookup -B ACLIENT '*'**. Sie sollten die IP-Adresse Ihres PCs erhalten. Wenn nicht, ist auf Ihrem PC die Software nicht richtig installiert, konfiguriert oder nicht gestartet oder Sie haben den Namen des PCs falsch eingegeben. Sollte ACLIENT keine DNS-Namensauflösung verwenden, dann benutzen Sie die IP-Adresse des Clients für den oben genannten Test.

6. Starten Sie den Befehl **nmblookup -d 2 '*'**. Dieses Mal versuchen wir dasselbe wie im vorigen Test, verwenden aber einen Broadcast über die Default-Broadcast-Adresse. Es sollten mehrere NetBios/TCP/IP-Rechner im Netzwerk antworten, obwohl Samba nicht alle Anworten in der kurzen Zeit erwischen kann. Sie sollten folgende Meldungen von diversen Hosts sehen: „*got a positive name query response*“. Sollten hier nicht die gleichen Ergebnisse wie im vorangegangenen Test erscheinen, dann erkennt nmblookup die korrekte Broadcast-Adresse nicht automatisch. In diesem Fall sollten Sie in `smb.conf` bei der interfaces-Option versuchen, die IP-Adresse, Broadcast-Adresse und Netzwerkmaske von Hand einzustellen. Befinden sich Ihr PC und Server in verschiedenen Subnetzen, benötigen Sie die `-B`-Option, um die Broadcast-Adresse des PC-Netzwerks zu benutzen. Dieser Test kann möglicherweise fehlschlagen, wenn Ihre Subnetz-Maske und Broadcast-Adresse nicht korrekt sind. (Siehe die Anmerkungen zu TEST 3).

7. Führen Sie folgenden Befehl aus: **smbclient //BIGSERVER/TMP**. Sie sollten nach einem Passwort gefragt werden. Verwenden Sie das Passwort Ihres aktuellen Accounts auf der Unix-Maschine. Möchten Sie den Test mit einem anderen Account durchführen, fügen Sie die Option `-U accountname` am Ende des Befehls hinzu, zum Beispiel **smbclient //bigserver/tmp -Ujohndoe**.

Anmerkung

Es ist folgendermaßen möglich, das Passwort zusammen mit dem Benutzernamen zu verwenden: **smbclient //bigserver/tmp -Ujohndoe%secret**.

Wenn Sie das Passwort eingegeben haben, erhalten Sie die `smb>`-Eingabeauforderung. Wenn nicht, beachten Sie die Fehlermeldung. Steht dort „*invalid network name*“, dann wurde die Freigabe *`tmp`* nicht korrekt in der `smb.conf` eingetragen. Steht dort „*bad password*“, dann könnte dies folgende Ursachen haben:

(a) Sie verwenden Shadow-Passwörter (oder ein anderes Passwort-System), haben aber keinen Support dafür in smbd einkompiliert.

(b) Ihr valid users-Eintrag ist nicht korrekt.

(c) Sie verwenden Groß-/Kleinschreibung im Passwort und haben die Option password level- nicht dementsprechend angepasst.

(d) Der path-Eintrag in `smb.conf` ist falsch. Überprüfen Sie dies mit testparm.

(e) Sie haben die Passwortverschlüsselung aktiviert, aber keine Unix-Benutzer zu Samba-Benutzern zugeordnet (gemappt). Starten Sie **smbpasswd -a username**.

Nachdem Sie verbunden sind, sollte es Ihnen möglich sein, die Befehle **dir**, **get**, **put** und so weiter aufzurufen. Näheres erfahren Sie durch **help command**. Sie sollten besonders die Anzeige des freien Festplattenplatzes mit **dir** überprüfen.

8. Führen Sie auf Ihrem PC in einer DOS-Eingabeaufforderung (DOS-Fenster) den Befehl **net view \\BIGSERVER** aus. Sie sollten eine Liste der verfügbaren Freigaben Ihres Servers erhalten. Erhalten Sie eine Meldung in der Art „*network name not found*“, dann funktioniert Ihre netbios-Namensauflösung nicht. Das ist überlicherweise ein Problem mit **nmbd**. Um das zu beheben, verwenden Sie eine der folgenden Möglichkeiten:

   (a) Korrigieren Sie die Installation von nmbd.

   (b) Fügen Sie die IP-Adresse von BIGSERVER zu den Einträgen des Felds **wins server** in der erweiterten TCP/IP- Konfiguration Ihres PCs hinzu.

   (c) Aktivieren Sie die Windows-Namensauflösung über DNS in der erweiterten Konfiguration des TCP/IP-Setups Ihres PCs.

   (d) Fügen Sie den Eintrag BIGSERVER zu Ihrer `lmhosts`-Datei auf dem PC hinzu.

   Erhalten Sie die Meldung „*invalid network name*“ oder „*bad password error*“, dann führen Sie dieselben Maßnahmen wie für die vorangegangenen **smbclient -L**-Tests durch. Achten Sie besonders darauf, ob die Einträge in **hosts allow** richtig sind (siehe die Manpages). Vergessen Sie bitte nicht, dass die Verbindungsanforderung von Ihrem PC zum Samba-Server immer mit dem aktuellen Benutzernamen Ihres angemeldeten Windows-Benutzers durchgeführt wird. Sie müssen sicherstellen, dass genau dieser

Benutzeraccount mit demselben Kennwort auch auf Ihrem Samba-Server existiert. Erhalten Sie eine Meldung in der Art „*specified computer is not receiving requests*“ , dann bedeutet dies vermutlich, dass der Computer nicht über TCP angesprochen werden kann. Wenn Ihr Computer TCP-Wrapper einsetzt, fügen Sie für den Client (oder das Subnetz usw.) einen Eintrag in die Datei `hosts.allow` hinzu.

9. Starten Sie den Befehl: **net use x: \\BIGSERVER\TMP**. Sie sollten nach einem Passwort gefragt werden und nach dessen Eingabe die Meldung `command completed successfully` erhalten. Sollte das nicht der Fall sein, ist Ihr PC nicht korrekt installiert oder die Datei `smb.conf` ist nicht in Ordnung. Stellen Sie sicher, dass die Einträge in *`hosts allow`* korrekt sind und die restlichen Einträge in `smb.conf` stimmen. Es ist auch möglich, dass der Server nicht erkennen kann, unter welchem Namen Sie sich verbinden. Um das Problem zu erkennen, fügen Sie die Zeile user = username im *`[tmp]`*-Abschnitt der `smb.conf` hinzu, wobei *`username`* der Benutzername zum eingegebenen Passwort sein muss. Wenn dass klappt, benötigen Sie die Option username mapping. Es ist auch möglich, dass Ihr Client nur verschlüsselte Passwörter versendet, aber der Eintrag encrypt passwords = no in der `smb.conf` steht. Ändern Sie diesen auf „*yes*“, um das Problem zu beheben.

10. Führen Sie den Befehl **nmblookup -M** *`testgroup`* aus, wobei *`testgroup`* der Name der Arbeitsgruppe Ihres Samba-Servers und Ihrer Windows-PCs ist. Sie sollten die IP-Adresse des Masterbrowsers für diese Arbeitsgruppe erhalten. Wenn nicht, dann ist der Auswahlprozess des Masterbrowsers fehlgeschlagen. Warten Sie evtl. noch ein paar Minuten, und versuchen Sie es dann nochmal, um zu sehen, ob es nur etwas langsam ist. Klappt es dann immer noch nicht, werfen Sie einen Blick auf die Browsing-Optionen in der `smb.conf`. Stellen Sie sicher, dass Sie preferred master = yes eingetragen haben, damit beim Starten eine Wahl des Masterbrowsers durchgeführt wird.

11. Durchsuchen Sie Ihre Netzwerkumgebung mit Ihrem Windows Explorer/Dateimanager. Ihr Samba-Server sollte in der Netzwerkumgebung unter Ihrer lokalen Arbeitsgruppe (oder der Arbeitsgruppe, die Sie in der `smb.conf` eingetragen haben) erscheinen. Es müsste Ihnen möglich sein, durch einen Doppelklick auf den Namen des Servers die Liste der Freigaben zu erhalten. Erhalten Sie eine Fehlermeldung „*invalid password*“, dann verwenden Sie möglicherweise Windows NT, denn NT öffnet keinen Server, der keine verschlüsselten Passwörter unterstützt und sich im User-Level-Security-Modus befindet. In diesem Fall tragen Sie security = server und password server = Windows_NT_Machine in Ihre `smb.conf` ein, oder stellen Sie sicher, dass encrypt passwords auf „*yes*“ steht.

Kapitel 33

ANALYSE UND LÖSUNG VON PROBLEMEN MIT SAMBA

Es gibt viele Informationsquellen in Form von Mailinglisten, RFCs und Dokumentation. Die Dokumentation, die mit der Samba-Distribution geliefert wird, enthält gute Erklärungen zu allgemeinen Samba-Themen wie Browsing.

33.1 Diagnose-Tools

Bei der Arbeit in Samba-Netzwerken ist es oft nicht sofort klar, was der Grund für ein bestimmtes Problem ist. Samba selbst bietet ziemlich hilfreiche Informationen an, aber in manchen Fällen werden Sie möglicherweise auf einen *Sniffer* zurückgreifen müssen. Ein Sniffer ist ein Programm, das in Ihrem LAN lauscht, die empfangenen Daten analysiert und sie auf dem Bildschirm anzeigt.

33.1.1 Das Debuggen mit Samba selbst

Eines der besten Diagnose-Tools, um Probleme zu debuggen, ist Samba selbst. Sie können die Option `-d` für smbd und nmbd verwenden, um den debug level festzulegen, auf dem sie ausgeführt werden sollen (siehe auch die Manpages für **smbd, nmbd** und `smb.conf` für mehr Informationen zu den Debugging-Optionen). Der Debug-Level reicht von 1 (Standard) bis zu 10 (100 zum Debuggen von Passwörtern).

Eine weitere hilfreiche Methode des Debugging ist es, Samba mit dem Flag **gcc -g** zu kompilieren. Dies wird Debug-Informationen in die Binaries mit einschließen, und erlaubt es, gdb an die laufenden **smbd/nmbd**-Prozesse anzudocken. Um dies auf einer NT-Workstation zu tun, lassen Sie zuerst die Workstation die Verbindung herstellen. Das Drücken von „*ctrl-alt-delete*“ und der Wechsel zum Domänen-Eintrag sollten ausreichen (zumindest beim ersten Anmelden an der Domäne), um den Parameter *`LsaEnumTrustedDomains`* zu generieren. Danach hält die Workstation eine offene Verbindung, und es wird ein smbd-Prozess laufen (vorausgesetzt, dass Sie keinen wirklich kurzen smbd-Timeout gesetzt haben). Also können Sie zwischen dem Drücken von **ctrl-alt-delete** und dem tatsächlichen Eingeben Ihres Passworts **gdb** starten und fortsetzen.

Einige Samba-Befehle, die nähere Betrachtung verdienen, sind:

```
$ testparm | more
$ smbclient -L //{Netbios-Name des Servers}
```

33.1.2 Tcpdump

Tcpdump <`http://www.tcpdump.org/`> war der erste UNIX-Sniffer mit SMB-Support. Es ist ein Befehlszeilen-Tool, und mittlerweile hängt seine SMB-Unterstützung etwas hinter der von **ethereal** und **tethereal** zurück.

33.1.3 Ethereal

Ethereal <`http://www.ethereal.com/`> ist ein grafischer Sniffer, der sowohl für UNIX (Gtk) als auch für Windows verfügbar ist. Ethereals SMB-Unterstützung ist ziemlich gut. Details zu **ethereal** finden Sie in dem gut geschriebenen Ethereal User Guide.

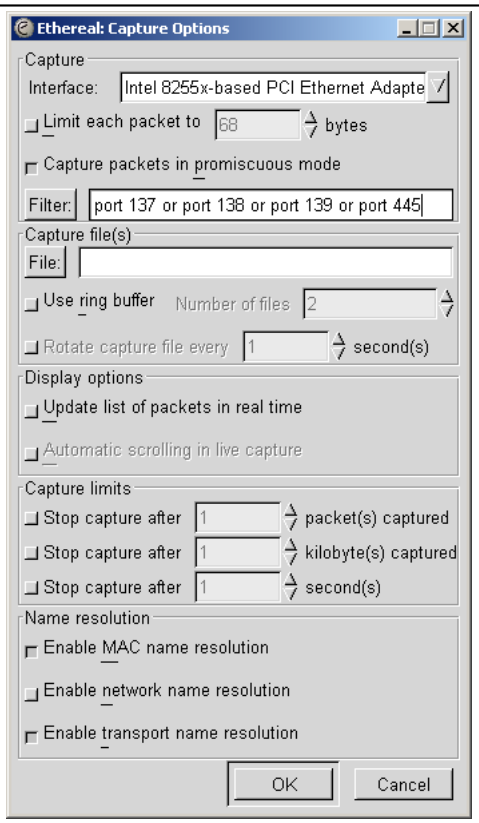


Figure 33.1. Start eines Capture

Überwachen Sie die Daten auf den Ports 137, 138, 139 und 445. Verwenden Sie beispielsweise den Filter `port 137`, `port 138`, `port 139` oder `port 445`, wie in Abbildung **??** zu sehen.

Eine Konsolenversion von ethereal ist auch verfügbar. Sie heißt **tethereal**.

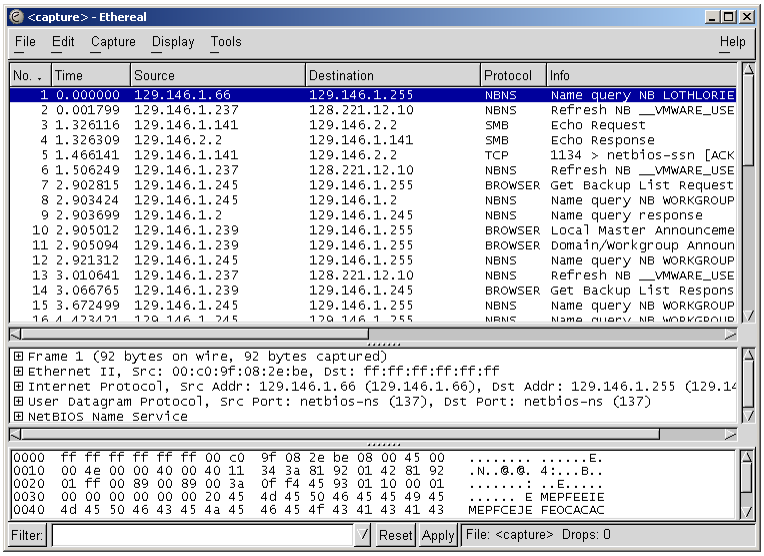

<capture> - Ethereal
File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
1 0.000000 129.146.1.66 129.146.1.255 NBNS Name query NB LOTHLORIE
2 0.001799 129.146.1.237 128.221.12.10 NBNS Refresh NB __VMWARE_USE
3 1.326116 129.146.1.141 129.146.2.2 SMB Echo Request
4 1.326309 129.146.2.2 129.146.1.141 SMB Echo Response
5 1.466141 129.146.1.141 129.146.2.2 TCP 1134 > netbios-ssn [ACK
6 1.506249 129.146.1.237 128.221.12.10 NBNS Refresh NB __VMWARE_USE
7 2.902815 129.146.1.245 129.146.1.255 BROWSER Get Backup List Request
8 2.903424 129.146.1.245 129.146.1.2 NBNS Name query NB WORKGROUP
9 2.903699 129.146.1.2 129.146.1.245 NBNS Name query response
10 2.905012 129.146.1.239 129.146.1.255 BROWSER Local Master Announceme
11 2.905094 129.146.1.239 129.146.1.255 BROWSER Domain/Workgroup Announ
12 2.921312 129.146.1.245 129.146.1.255 NBNS Name query NB WORKGROUP
13 3.010641 129.146.1.237 128.221.12.10 NBNS Refresh NB __VMWARE_USE
14 3.066765 129.146.1.239 129.146.1.245 BROWSER Get Backup List Respons
15 3.672499 129.146.1.245 129.146.1.255 NBNS Name query NB WORKGROUP
Frame 1 (92 bytes on wire, 92 bytes captured)
Ethernet II, Src: 00:c0:9f:08:2e:be, Dst: ff:ff:ff:ff:ff:ff
Internet Protocol, Src Addr: 129.146.1.66 (129.146.1.66), Dst Addr: 129.146.1.255 (129.14
User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
NetBIOS Name Service
0000 ff ff ff ff ff ff 00 c0 9f 08 2e be 08 00 45 00 ....E.
0010 00 4e 00 00 40 00 40 11 34 3a 81 92 01 42 81 92 .N..@.@. 4:...B..
0020 01 ff 00 89 00 89 00 3a 0f f4 45 93 01 10 00 01 .....: ..E.....
0030 00 00 00 00 00 00 20 45 4d 45 50 46 45 45 49 45 ..... E MEPFEEIE
0040 4d 45 50 46 43 45 4a 45 46 45 4f 43 41 43 41 43 MEPFCEJE FEOCACAC
Filter: Reset Apply File: <capture> Drops: 0

Figure 33.2. Hauptansicht von ethereal

33.1.4 Der Windows Netzwerk-Monitor

Um Dinge unter Microsoft Windows NT zu verfolgen, verwenden Sie den Netzwerk-Monitor (auch bekannt als Netmon) von den Microsoft Developer Network-CDs. Er ist auch auf der Installations-CD des Windows NT-Servers und auf den SMS-CDs enthalten. Die mit SMS gelieferte Version erlaubt es, Pakete zwischen zwei Rechnern zu dumpen (d.h., die Netzwerkkarte im Promiscuous Mode zu betreiben). Die Version auf der Windows NT Server-CD erlaubt nur das Monitoring von Netzwerkverkehr zur lokalen NT-Maschine und Broadcasts im lokalen Subnetz. Beachten Sie, dass Ethereal Dateien im Netmon-Format lesen und schreiben kann.

33.1.4.1 Installieren des Netzwerk-Monitors auf einer NT-Workstation

Das Installieren von Netmon auf einer NT-Workstation erfordert einige Schritte. Die folgenden Anweisungen gelten für die Installation von Netmon V4.00.349, der mit dem Microsoft Windows NT Server 4.0 geliefert wird, auf Microsoft Windows NT Workstation 4.0. Der Ablauf sollte für andere Versionen von Netmon für Windows NT ähnlich sein. Sie werden sowohl die NT Server 4.0-Installations-CD als auch die Workstation 4.0 Installations-CD dazu brauchen.

Zuerst müssen Sie Network Monitor Tools and Agent auf dem NT-Server installieren:

- Gehen Sie auf **Start** -> **Settings** -> **Control Panel** -> **Network** -> **Services** -> **Add**.

- Wählen Sie **Network Monitor Tools and Agent**, und klicken Sie auf **OK**.
- Klicken Sie im Network Control Panel auf **OK**.
- Legen Sie die NT Server 4.0-Installations-CD ein, wenn Sie dazu aufgefordert werden.

An diesem Punkt sollten die Netmon-Dateien in `%SYSTEMROOT%\System32\netmon\*.*` existieren. Es gibt auch zwei Unterverzeichnisse: `parsers\`, das die notwendigen DLLs enthält, um den Netmon-Paket-dump zu parsen, und `captures\`.

Um die Netmon-Tools auf einer NT-Workstation zu installieren, müssen Sie zuerst den Network Monitor Agent von der Workstation 4.0-Installations-CD installieren.

- Gehen Sie auf **Start** -> **Settings** -> **Control Panel** -> **Network** -> **Services** -> **Add**.
- Wählen Sie **Network Monitor Agent**, und klicken Sie auf **OK**.
- Klicken Sie im Network Control Panel auf **OK**.
- Legen Sie die NT Server 4.0-Installations-CD ein, wenn Sie dazu aufgefordert werden.

Kopieren Sie jetzt die Dateien vom NT Server in `%SYSTEMROOT%\System32\netmon` nach `%SYSTEMROOT%\System32\netmon` auf der Workstation, und setzen Sie die Berechtigungen so, wie Sie sie für Ihre Installation angemessen halten. Sie brauchen Administrator-Rechte auf der NT-Maschine, um Netmon auszuführen.

33.1.4.2 Installieren des Netzwerk-Monitors unter Windows 9x/Me

Um Netmon unter Windows 9x/Me zu installieren, installieren Sie den Network Monitor Agent von der Windows 9x/Me-CD (`\admin\nettools\netmon`). Es gibt eine README-Datei bei den Netmon-Treiber-Dateien auf der CD, wenn Sie Informationen dazu brauchen. Kopieren Sie die Dateien von einer bestehenden Netmon-Installation.

33.2 Hilfreiche URLs

- Sehen Sie, wie Scott Merrill das Verhalten eines BDCs simuliert: http://www.skippy.net/linux/smb-howto.html <`http://www.skippy.net/linux/smb-howto.html`>.
- Eine FTP-Site für ältere SMB-Spezifikationen ist: ftp://ftp.microsoft.com/developr/drg/CIFS/ <`ftp://ftp.microsoft.com/developr/drg/CIFS/`>

33.3 Hilfe aus Mailing-Listen erhalten

Es gibt eine Anzahl von Mailinglisten im Zusammenhang mit Samba. Gehen Sie auf <`http://samba.org`>, klicken Sie auf Ihren nächsten Mirror, dann auf **Support** und auf **Samba-related mailing lists**.

Für Fragen im Zusammenhang mit Samba-TNG, einer speziellen Version von Samba, gehen Sie auf http://www.samba-tng.org/. <`http://www.samba-tng.org/`> Es wurde darum gebeten, Fragen zu Samba-TNG nicht in die Mainstream-Samba-Listen zu posten.

Wenn Sie eine Nachricht an eine der Listen senden, beachten Sie bitte folgende Richtlinien:

- Erinnern Sie sich immer daran, dass die Entwickler Freiwillige sind. Sie werden nicht bezahlt, und sie garantieren niemals, ein bestimmtes Feature in einer bestimmten Zeit zu produzieren. Alle Zeitangaben sind „*Schätzwerte*“ und nicht mehr.
- Erwähnen Sie immer, welche Version von Samba Sie einsetzen und unter welchem Betriebssystem diese läuft. Sie sollten die relevanten Abschnitte Ihrer `smb.conf`-Datei auflisten, zumindest die Optionen in `[global]`, die den PDC-Betrieb beeinflussen.
- Wenn Sie Samba via SVN (Subversion) bezogen haben, erwähnen Sie bitte zusätzlich zur Version das Datum, an dem Sie zuletzt ein „*svn checkout*“ durchgeführt haben.
- Versuchen Sie, Ihre Fragen klar und kurz zu halten. Viele langatmige Konvolute werden gelöscht, bevor sie überhaupt ganz gelesen werden! Senden Sie keine HTML-codierten Nachrichten. Die meisten Leute auf Mailing-Listen löschen diese einfach.
- Wenn Sie eines dieser hübschen „*Ich bin auf Urlaub!*“-Dinger verwenden, während Sie weg sind, stellen Sie sicher, dass es so konfiguriert ist, nicht auf Mailinglisten-Verkehr zu antworten. Auto-Responses auf Mailinglisten ärgern Tausende Leute, die mit solch schlechter Netiquette konfrontiert werden.
- Vermeiden Sie das „*Cross-Posting*“. Finden Sie heraus, welche die beste Liste für Ihre Fragen ist, und sehen Sie, was passiert. Posten Sie nicht in den Listen `samba` UND `samba-technical`. Viele der Leute, die in diesen Listen aktiv sind, haben mehrere Listen abonniert und ärgern sich darüber, dieselbe Nachricht zweimal oder noch öfter zu sehen. Oft wird jemand eine Nachricht sehen, sich denken, dass diese besser in einer anderen Liste behandelt würde, und die Nachricht für Sie weiterleiten.
- Sie könnten *auszugsweise* Log-Dateien einschließen, die auf einem Debug-Level bis zu 20 geschrieben wurden. Bitte senden Sie nicht die ganze Log-Datei, sondern nur so viel, um den Kontext für die Fehlermeldungen zu schaffen.
- Wenn Sie einen kompletten Netmon-Trace haben (vom Öffnen der Pipe bis zum Fehler), können Sie auch die *.CAP-Datei senden.
- Bitte überlegen Sie sorgfältig, bevor Sie ein Dokument an eine E-Mail hängen. Erwägen Sie, die relevanten Teile in die E-Mail zu kopieren. Die Samba-Mailing-Listen gehen an eine riesige Zahl von Menschen. Brauchen diese alle eine Kopie Ihrer `smb.conf` in ihrem Attachment-Verzeichnis?

33.4 Wie man aus Mailinglisten rauskommt

Um Ihren Namen von einer Samba-Mailingliste löschen zu lassen, gehen Sie dorthin, wo Sie ihn in die Liste haben eintragen lassen. Gehen Sie auf http://lists.samba.org <`http://lists.samba.org/`>, klicken Sie auf Ihren nächsten Mirror, klicken Sie auf **Support** und dann auf **Samba related mailing lists**.

Bitte senden Sie keine Nachrichten an die Liste, in denen Sie darum bitten, von der Liste entfernt zu werden. Sie werden nur an obige Adresse verwiesen werden (außer dieser Prozess ist aus irgendeinem Grund gescheitert).

Kapitel 34

DAS MELDEN VON FEHLERN

34.1 Einführung

Bitte verwenden Sie Bugzilla <`https://bugzilla.samba.org/`>, um Bugs zu melden, und lesen Sie zunächst dieses Kapitel, bevor Sie einen Bug melden. Bitte prüfen Sie gleichfalls, ob sich dieser Text nach einem Releasewechsel geändert hat, da wir an einigen Punkten den Mechanismus zum Thema Bug-Report ändern.

Bitte geben Sie so viele Informationen in dem Bug-Report an, wie Sie können. Wir bekommen täglich mehr Mails, als wir beantworten können, also helfen Sie uns bitte, indem Sie Ihren Bug so „*entwickler-freundlich*“ wie nur eben möglich beschreiben.

Bitte gehen Sie nicht davon aus, dass wir, wenn Sie einen Bug in der Newsgroup comp.protocols.smb posten, diese Nachricht lesen. Wenn Sie vermuten, dass es weniger ein Bug als ein Konfigurationsproblem ist, wenden Sie sich bitte an die Samba-Mailingliste, da dort Tausende von anderen Benutzern evtl. in der Lage sind, Ihnen zu helfen.

Ebenfalls hilfreich ist ein Durchsuchen der Mailinglisten-Archive, die über die Samba-Webseite <`http://samba.org/samba/`> zu erreichen sind.

34.2 Allgemeine Informationen

Bevor Sie einen Bug-Report senden, prüfen Sie bitte Ihre Konfiguration auf Tippfehler. Sehen Sie sich auch Ihre Log-Dateien daraufhin an, ob diese ggf. eine Nachricht anzeigen, dass etwas falsch konfiguriert worden ist. Um die Syntax Ihrer Konfiguration zu prüfen, führen Sie bitte testparm aus.

Haben Sie in Kapitel **??** „Die Samba-Checkliste“ nachgeschaut? Dies ist absolut wichtig!

Wenn Sie Teile Ihrer Log-Dateien mit dem Report senden, stellen Sie sicher, dass Sie sie entsprechend Ihrer Tätigkeit am Client kommentieren und und mitteilen, wie sich das Resultat darstellt.

34.3 Debug-Level

Wenn der Bug etwas damit zu tun hat, dass sich Samba als Server inkorrekt verhält (etwa es ablehnt, eine Datei zu öffnen), sind die Log-Dateien sehr nützlich. Je nach Problem ist ein Log-Level zwischen 3 und 10 sehr hilfreich, um das Problem zu analysieren. Ein höherer Log Level verspricht mehr Detail-Informationen, benötigt allerdings auch mehr Speicherkapazität.

Um den Debug-Level einzustellen, verwenden Sie die Option log level in Ihrer `smb.conf`. Es ist nützlich, für jede Maschine eine eigene Log-Datei zu verwenden und nur für eine Maschine den Log-Level höher einzustellen. Wenn Sie dies machen möchten, fügen Sie bitte folgende Zeilen zu Ihrer `smb.conf` hinzu:

```
log level = 10
log file = /usr/local/samba/lib/log.%m
include = /usr/local/samba/lib/smb.conf.%m
```

Erstellen Sie außerdem eine Datei `/usr/local/samba/lib/smb.conf.`*machine*, wobei *machine* der Name des Clients ist, den Sie debuggen wollen. In dieser Datei können Sie alle `smb.conf`-Optionen setzen, zum Beispiel ist das Setzen des Parameters log level nützlich. Hier können Sie auch mit verschiedenen Sicherheitsoptionen experimentieren.

Der `smb.conf`-Eintrag log level ist ein Synonym für debuglevel, der in älteren Versionen von Samba verwendet wurde und dazu dient, die Abwärtskompatibilität zu älteren `smb.conf`-Dateien zu gewährleisten.

Sobald der Wert für den log level erhöht und Samba neu gestartet worden ist, werden Sie eine signifikant größere Menge an Debug-Informationen erhalten. Für gewöhnlich werden Sie keinen Level höher als `3` benötigen. Nahezu jeder Bug kann mit einem Log-Level von `10` festgestellt werden, aber machen Sie sich auf ein großes Datenvolumen an Log-Dateien gefasst.

34.4 Interne Fehler

Wenn Sie in Ihren Log-Dateien einen „*INTERNAL ERROR*“ bemerken sollten, bedeutet dies, dass Samba ein nicht erwartetes Signal bekommen hat. Dies ist wahrscheinlich ein „*segmentation fault*“ und deutet so gut wie sicher auf einen Bug in Samba hin (vorausgesetzt, Ihre Hardware oder Systemsoftware funktioniert einwandfrei).

Sollte die Nachricht vom smbd stammen, ist es meistens so, dass vor dieser Nachricht das Log noch die letzte SMB-Meldung enthält, die der smbd erhalten hat. Diese Information ist oft sehr nützlich, um das Problem zu lokalisieren: Bitte fügen Sie daher diese Meldung Ihrem Bug-Report hinzu.

Falls möglich sollten Sie so detailliert wie möglich erklären können, wie das Problem reproduziert werden kann.

Sie werden ebenfalls eine so genannte Core-Datei in einem `corefiles` -Unterverzeichnis in Ihrem Log-Verzeichnis entdecken. Diese Datei ist das nützlichste Tool, um einen Bug zu verfolgen. Um es zu verwenden, machen Sie Folgendes:

```
$ gdb smbd core
```

Fügen Sie die jeweiligen Pfade zu smbd und der Core-Datei zu gdb hinzu, damit gdb sie finden kann. Wenn Sie gdb nicht haben sollten, versuchen Sie es mit `dbx`. Anschließend verwenden Sie innerhalb des Debuggers das Kommando **where**, um einen stack-Trace der Stelle zu erhalten, an der das Problem auftrat. Fügen Sie diese Information der Bug-Meldung hinzu.

Wenn Sie Kenntnisse in einer Assembler-Sprache haben, führen Sie ein **disass**-Kommando zu der Routine hinzu, in der das Problem auftrat (wenn es in einer Library-Routine war, disassemblieren Sie die Routine, die sie aufgerufen hat), und versuchen Sie festzustellen, an welcher Stelle das Problem liegt, indem Sie sich den Code ansehen. Selbst wenn Sie keine Kenntnisse in Assembler-Programmierung haben, sollten Sie diese Information dem Report hinzufügen, dies kann sehr hilfreich sein.

34.5 Sich an einen laufenden Prozess anschließen

Leider lassen es einige UNIX-Varianten (zum Teil auch einige Linux-Kernel) nicht zu, einen Coredump zu erstellen, wenn der Prozess die UID ändert (was smbd oft tut). Um dies dennoch zu debuggen, könnten Sie versuchen, sich in den laufenden Prozess einzuklinken, indem Sie `gdb smbd` *`PID`* ausführen, wobei Sie die *`PID`* aus dem smbstatus entnehmen können. Anschließend verwenden Sie das **c**-Kommando, um fortzufahren und um zu versuchen, den Coredump mit Hilfe des Clients zu erzeugen. Der Debugger sollte den Fehler erfassen und Ihnen mitteilen, wo er auftrat.

34.6 Patches

Die beste Art von Bug-Reports sind die, die bereits einen Fix beinhalten! Wenn Sie uns Patches schicken, verwenden Sie bitte das `diff -u`-Format, wenn Ihre Version von diff dies bereitstellt. Ansonsten verwenden Sie bitte `diff -c4`. Stellen Sie sicher, dass Sie Ihr diff gegen eine saubere Version des Source-Codes erstellen, und lassen Sie uns wissen, welche Version genau Sie verwenden.

Teil VI

Anhang

Kapitel 35

WIE MAN SAMBA KOMPILIERT

Der Source-Text von Samba kann von der Samba-Website <`http://samba.org/`> bezogen werden. Um eine Entwicklerversion zu beziehen, können Sie Samba mit CVS oder **rsync** herunterladen.

35.1 Der Zugriff auf den Source-Code von Samba über Subversion

35.1.1 Einführung

Samba wird in einer offenen Umgebung entwickelt. Die Entwickler benutzen Subversion (SVN), um mit „*checkin*“ (das auch als „*commit*“ bekannt ist) neuen Quelltext einzufügen. Sie können auf die verschiedenen SVN-Zweige von Samba mit anonymem SVN zugreifen werden, wenn Sie die Anleitungen befolgen, die in diesem Kapitel enthalten sind.

Dieses Kapitel ist eine geänderte Fassung der Instruktionen, die Sie auf der Samba <`http://samba.org/samba/subversion.html`>-Website finden.

35.1.2 Der Subversion-Zugriff auf samba.org

Die Maschine samba.org führt ein offen zugängliches Subversion-Repository aus. Damit ermöglicht sie den Zugriff auf den Quelltext mehrerer Packages, einschließlich Samba, rsync, distcc, ccache und jitterbug. Es gibt zwei hauptsächliche Arten, um auf den Subversion-Server auf diesem Host zuzugreifen:

35.1.2.1 Zugriff via SVNweb

Sie können unter Verwendung Ihres bevorzugten WWW-Browsers auf den Quelltext zugreifen. Auf diese Weise können Sie sowohl auf einzelne Dateien im Repository als auch auf den Verlauf der Revisionen und die Commit-logs der einzelnen Dateien zugreifen. Sie können damit auch diff-Listings zwischen zwei Versionen erstellen.

Verwenden Sie die URL <`http://svnweb.samba.org/`>

35.1.2.2 Zugriff via Subversion

Sie können auf den Quelltext auch mit einem normalen Subversion-Client zugreifen. Dies gibt Ihnen mehr Kontrolle darüber, was Sie mit dem Repository tun können, und erlaubt Ihnen, ganze Quelltext-Bäume mit **checkout** abzuholen und sie mittels normaler SVN-Befehle aktuell zu halten. Dies ist die bevorzugte Variante des Zugriffs, wenn Sie ein Entwickler und nicht nur ein gelegentlicher Besucher sind.

Um die Samba-Quelltexte von Subversion herunterladen zu können, brauchen Sie einen Subversion-Client. Ihre Distribution kann einen solchen enthalten, oder Sie laden sich die Quelltexte von <`http://subversion.tigris.org/`> herunter.

Um einen anonymen Zugriff mit Subversion zu erlangen, führen Sie die folgenden Schritte durch. In diesem Beispiel wird angenommen, dass Sie eine Kopie des Samba-Quelltexts haben wollen. Für die anderen Quelltext-Repositories auf diesem System ersetzen Sie einfach den Package-Namen. Samba über Subversion beziehen

1. Installieren Sie eine aktuelle Version von Subversion. Sie brauchen dazu nur eine Kopie des Subversion-Client-Programms.
2. Führen Sie folgenden Befehl aus: `svn co svn://svnanon.samba.org/samba/trunk samba`. Dies legt ein Verzeichnis namens `samba` an, das den neuesten Samba-Quellcode enthält (üblicherweise den Zweig, der zur nächsten Haupt-Release werden soll). Dies entspricht derzeit dem 3.1-Entwicklungsbaum. Subversion-Zweige, die nicht dem TRUNK entsprechen, können Sie durch Anhängen von branches/BRANCH_NAME an die URL auschecken. Eine Liste von Branch-Namen finden Sie auf der „*Development*“-Seite der Samba-Website. Eine gebräuchliche Anfrage ist die nach dem letzten 3.0-Release-Code. Dies könnte wie folgt geschehen: `svn co svn://svnanon.samba.org/samba/branches/SAMBA_3_0 samba_3`.
3. Wenn Sie die letzten Code-Änderungen übernehmen wollen, verwenden Sie folgenden Befehl innerhalb des Samba-Verzeichnisses: `svn update`

35.2 Zugriff auf die Samba-Quelltexte mit rsync und ftp

pserver.samba.org exportiert auch ungepackte Kopien der meisten Teile des CVS-Baums unter <`ftp://pserver.samba.org/pub/unpacked`> und auch mit anonymem rsync unter <`rsync://pserver.samba.org/ftp/unpacked/`>. Wir empfehlen, rsync statt ftp zu verwenden. Sehen Sie sich die rsync-Homepage <`http://rsync.samba.org/`> an, um mehr Informationen zu rsync zu erhalten.

Der Nachteil der ungepackten Bäume ist, dass sie kein automatisches „*Merging*“ von lokalen Änderungen zulassen, wie es CVS tut. Der **rsync**-Zugriff ist das praktischste Verfahren bei einer frischen Installation.

35.3 Überprüfen der PGP-Signatur von Samba

Wir empfehlen, unbedingt die PGP-Signatur jeder Quelltext-Datei vor der Installation zu überprüfen. Selbst wenn Sie die Datei nicht von einem Mirror-Server laden, sollte das Prüfen

der PGP-Signatur zum Reflex werden. Viele nutzen heute das GNU-GPG-Package anstelle von PGP. GPG kann statt PGP eingesetzt werden.

Nachdem wir dies geklärt haben, laden Sie nun bitte folgende Dateien aus dem Netz:

```
$ wget http://us1.samba.org/samba/ftp/samba-2.2.8a.tar.asc
$ wget http://us1.samba.org/samba/ftp/samba-pubkey.asc
```

Die erste Datei ist die PGP-Signatur für die Samba-Quelltext-Datei; die andere ist der öffentliche Samba-PGP-Schlüssel selbst. Importieren Sie den öffentlichen PGP-Schlüssel mit

```
$ gpg --import samba-pubkey.asc
```

und überprüfen Sie die Integrität des Samba-Quelltexts mit:

```
$ gzip -d samba-2.2.8a.tar.gz
$ gpg --verify samba-2.2.8a.tar.asc
```

Wenn Sie eine Meldung wie „*Good signature from Samba Distribution Verification Key...*“ erhalten, ist alles in Ordnung. Die Warnungen bezüglich „*trust relationships*“ können Sie ignorieren. Ein Beispiel für etwas, das Sie nicht sehen wollen, wäre:

```
gpg: BAD signature from Samba Distribution Verification Key
```

35.4 Kompilieren der Binärdateien

Um die Binärdateien mittels „*build*“ zu erhalten, führen Sie zuerst das Programm `./configure` im Quellverzeichnis aus. Dies sollte Samba automatisch für Ihr Betriebssystem konfigurieren. Sollten Sie darüber hinausgehende Wünsche haben, dann können Sie Folgendes angeben:

```
root# ./configure --help
```

So sehen Sie, welche speziellen Optionen aktiviert werden können. Nun können Sie `./configure` mit allen gewünschten Agrumenten ausführen:

```
root# ./configure [... arguments ...]
```

Das Ausführen von

```
root# make
```

wird die Binärdateien erstellen. Sobald diese erfolgreich kompiliert worden sind, können Sie

```
root# make install
```

verwenden, um die Binärdateien (= Programme) und Manpages zu installieren. Sie können Programme und Manpages separat installieren:

```
root# make installbin
```

und

```
root# make installman
```

Bitte beachten Sie: Beim Upgrade von einer vorigen Version werden die alten Programme umbenannt, und zwar durch das Anhängen von „*.old*“. Sie können dann mit

```
root# make revert
```

zur alten Version zurückkehren, wenn Sie die neue Version als Desaster empfinden!

35.4.1 Das Kompilieren von Samba mit Active Directory Support

Um Samba mit ADS-Support zu kompilieren, müssen Sie Folgendes auf Ihrem System installiert haben:

- Die MIT- oder Heimdal-Kerberos-Entwickler-Bibliotheken (entweder selbst kompiliert oder aus einem Package)
- Die OpenLDAP-Entwickler-Bibliotheken

Wenn Ihre Kerberos-Bibliotheken an einem vom Standard-Verzeichnis abweichenden Ort liegen, fügen Sie die Konfigurationsoption `--with-krb5=`*`DIR`* hinzu.

Nachdem Sie **configure** ausgeführt haben, prüfen Sie, ob die entstandene Datei `include/config.h` Zeilen wie diese enthält:

```
#define HAVE_KRB5 1
#define HAVE_LDAP 1
```

Falls dem nicht so ist, hat **configure** Ihre KRB5-Libraries oder LDAP-Libraries nicht gefunden. Konsultieren Sie `config.log`, um den Grund dafür zu finden und zu beheben.

35.4.1.1 Die Installation der für Debian erforderlichen Packages

Unter Debian müssen Sie folgende Packages installieren:

- libkrb5-dev
- krb5-user

35.4.1.2 Die Installation der für Red Hat Linux erforderlichen Packages

Unter Red Hat Linux brauchen Sie zusätzlich zur Standard-Entwicklungsumgebung zumindest Folgendes:

- krb5-workstation (für kinit)
- krb5-libs (für das Linken)
- krb5-devel (weil Sie aus den Quellen kompilieren)

Wenn diese Dateien nicht auf Ihrem System installiert sind, sollten Sie die Installations-CDs überprüfen, um herauszufinden, wo diese Packages zu finden sind, und sie mit einem Werkzeug Ihrer Wahl installieren. Wenn Sie unsicher sind, welches Werkzeug zu verwenden ist, lesen Sie bitte die Red Hat Linux-Dokumentation.

35.4.1.3 Package-Anforderungen in SuSE Linux

SuSE Linux installiert Heimdal-Packages, die erforderlich sein könnten, um Binary-Packages erstellen zu können. Sie sollten überprüfen, ob diese Entwickler-Bibliotheken auf Ihrem System installiert worden sind.

SuSE Linux-Samba-RPMs unterstützen Kerberos. Bitte sehen sie in die Dokumentation Ihres SuSE Linux-Systems, wenn Sie Informationen zur SuSE-spezifischen Konfiguration brauchen. Außerdem ist SuSE sehr aktiv, was die Pflege von Samba-Packages betrifft, die alle verfügbaren Fähigkeiten von Samba bereitstellen. Sie sollten die Verwendung von SuSE-Samba-Packages in Erwägung ziehen, falls dies möglich ist.

35.5 Starten von smbd und nmbd

Sie müssen sich entscheiden, smbd und nmbd entweder als „*Daemons*“ oder mit inetd zu starten. Versuchen Sie nicht, beides zu tun! Sie können sie entweder in `inetd.conf` eintragen und bei Bedarf von inetd oder xinetd starten lassen, oder sie als Daemons entweder von der Befehlszeile oder in `/etc/rc.local` starten. Lesen Sie die Manpages für Details zu den Befehlsoptionen. Lesen Sie im Besonderen den Abschnitt über den Benutzer, den Sie brauchen, um Samba zu starten. In vielen Fällen müssen Sie dazu root sein.

Der hauptsächliche Vorteil des Startens von smbd und nmbd mit der empfohlenen Daemon-Methode ist, dass sie dann etwas schneller auf die erste Verbindungsanfrage reagieren werden.

35.5.1 Starten aus der inetd.conf

ANMERKUNG

Das Folgende ist unterschiedlich, je nachdem, ob Sie NIS, NIS+ oder LDAP zur Verteilung Ihrer Dienst-Listen verwenden.

Sehen Sie sich `/etc/services` an. Was ist für Port 139 (TCP) definiert? Wenn nichts definiert ist, fügen Sie eine Zeile wie diese hinzu:

```
netbios-ssn     139/tcp
```

Ähnliches gilt für Port 137 (UDP). Sie sollten einen Eintrag haben wie:

```
netbios-ns  137/udp
```

Als Nächstes editieren Sie Ihre `/etc/inetd.conf` und fügen zwei Zeilen wie diese hinzu:

```
netbios-ssn stream tcp nowait root /usr/local/samba/bin/smbd smbd
      netbios-ns dgram udp wait root /usr/local/samba/bin/nmbd nmbd
```

Die exakte Syntax von `/etc/inetd.conf` variiert zwischen den einzelnen UNIX-Varianten. Nehmen Sie sich einfach andere Einträge in der inetd.conf zur Vorlage.

Manche Distributionen verwenden xinetd anstatt von inetd. Konsultieren Sie das xinetd-Manual für Informationen zur Konfiguration.

ANMERKUNG

Manche UNIX-Varianten haben bereits Einträge wie netbios_ns (beachten Sie den Unterstrich) in `/etc/services`. Sie müssen `/etc/services` oder `/etc/inetd.conf` editieren, um beide konsistent zu halten.

ANMERKUNG

Auf vielen Systemen müssen Sie eventuell die Option interfaces in `smb.conf` verwenden, um die IP-Adresse und die Netzmaske Ihrer Netz-Interfaces anzugeben. Führen Sie ifconfig als root aus, wenn Sie die Broadcast-Adresse Ihres Netzes nicht kennen. nmbd versucht diese bei seiner Ausführung zu bestimmen, scheitert aber auf manchen UNIX-Varianten.

WARNUNG

Viele UNIX-Varianten akzeptieren nur ungefähr fünf Parameter auf der Befehlszeile in `inetd.conf`. Das bedeutet, dass Sie keine Leerzeichen zwischen Optionen und Argumenten verwenden sollten bzw. dass Sie ein Skript verwenden und dies mit **inetd** starten sollten.

Starten Sie inetd neu bzw. senden Sie das Signal HUP.

```
root# killall -HUP inetd
```

35.5.2 Alternative: smbd als Daemon starten

Um den Server als Daemon zu starten, sollten Sie ein Skript wie das Folgende anlegen, zum Beispiel mit dem Namen `startsmb`:

```
#!/bin/sh
/usr/local/samba/bin/smbd -D
/usr/local/samba/bin/nmbd -D
```

Machen Sie es mit **chmod +x startsmb** ausführbar.

Dann können Sie **startsmb** von Hand oder in der Datei `/etc/rc.local` starten.

Um die Daemons zu beenden, senden Sie ein KILL-Signal an die Prozesse nmbd und smbd.

ANMERKUNG

Wenn Sie das init-System in der Art von SVR4 verwenden, wollen Sie vielleicht das Beispiel-Skript `examples/svr4-startup` lesen, um Samba an Ihr System anzupassen.

Kapitel 36

PORTABILITÄT

Samba arbeitet auf einer Vielzahl von Plattformen, aber das Interface, das diese Plattformen bereitstellen, ist nicht immer kompatibel. Dieses Kapitel enthält plattform-spezifische Information über das Kompilieren und die Verwendung von Samba.

36.1 HPUX

Die HP-Implementation von unterstützenden Gruppen ist (aus historischen Gründen) nicht standardkonform. Es gibt zwei Gruppen-Dateien, `/etc/group` und `/etc/logingroup`. Das System mappt UIDs auf Nummern unter Verwendung der ersten Datei, aber initgroups() liest letztere. Die meisten System-Admins, die die Regeln kennen, linken `/etc/group` auf `/etc/logingroup` mit einem Symlink (Hardlinks funktionieren hier nicht; die Gründe zu erläutern, würde hier zu weit führen). nitgroups() wird sich beschweren, wenn eine der Gruppen, zu denen Sie gehören, in `/etc/logingroup` eine ID hat, die es für ungültig hält, was bedeutet, dass sie außerhalb des Bereichs `[0..UID_MAX]` liegt, wobei `UID_MAX` momentan (glaube ich) unter HP-UX 60000 beträgt. Dies schließt -2 und 65534 aus, die üblichen GIDs für `nobody`.

Wenn Ihnen dieses Problem begegnet, stellen Sie sicher, dass die Programme, die beim Aufruf von initgroups() scheitern, als Benutzer ausgeführt werden, nicht in Gruppen, deren GIDs außerhalb des erlaubten Bereichs liegen.

Dies ist in den HP-Manpages von setgroups(2) und passwd(4) dokumentiert.

Unter HP-UX müssen Sie gcc oder den HP ANSI-Compiler verwenden. Der freie Compiler, der HP-UX beiliegt, entspricht nicht ANSI und kann Samba nicht kompilieren.

36.2 SCO UNIX

Wenn Sie eine alte Version von SCO UNIX verwenden, kann es sein, dass Sie wichtige TCP/IP-Patches brauchen, damit Samba korrekt arbeitet. Ohne die Patches können beschädigte Daten-Transfers mit Samba auftreten.

Der Patch, den Sie brauchen, ist „*UOD385 Connection Drivers SLS*“. Er ist verfügbar bei SCO (ftp.sco.com <`ftp://ftp.sco.com/`>, Verzeichnis SLS, Dateien uod385a.Z und

uod385a.ltr.Z).

Die hier gegebene Information bezieht sich auf eine alte Version von SCO UNIX. Wenn Sie Binaries für neuere SCO UNIX-Produkte brauchen, kontaktieren Sie bitte SCO, um installationsfähige Pakete zu beziehen. Sie sollten außerdem mit SCO prüfen, ob Ihre Plattform up-to-date für die Pakete ist, die Sie installieren wollen. Dies ist wichtig, um eine Beschädigung von Daten durch die Installation zu vermeiden. Um Samba für SCO UNIX-Produkte zu kompilieren, kann es notwendig sein, Samba umfangreich zu patchen. Es ist deutlich einfacher, fertige Binary-Pakete direkt von SCO zu beziehen.

36.3 DNIX

DNIX hat ein Problem mit **seteuid()** und **setegid()**. Diese Routinen werden für den korrekten Betrieb von Samba gebraucht, wurden aber in der DNIX-C-Library aus irgendeinem Grund weggelassen.

Aus diesem Grund definiert Samba per Default das Makro NO_EID im DNIX-Abschnitt von includes.h. Dies umgeht das Problem in eingeschränkter Weise, ist aber bei weitem nicht ideal, und einige Dinge werden nach wie vor nicht richtig arbeiten.

Um das Problem sauber zu lösen, müssen Sie die folgenden zwei Funktionen zusammenbauen und sie dann entweder Ihrer C-Library hinzufügen oder sie in Samba linken. Schreiben Sie Folgendes in die Datei `setegid.s`:

```
        .globl  _setegid
_setegid:
        moveq   #47,d0
        movl    #100,a0
        moveq   #1,d1
        movl    4(sp),a1
        trap    #9
        bccs    1$
        jmp     cerror
1$:
        clrl    d0
        rts
```

Schreiben Sie Folgendes in die Datei `seteuid.s`:

```
        .globl  _seteuid
_seteuid:
        moveq   #47,d0
        movl    #100,a0
        moveq   #0,d1
        movl    4(sp),a1
        trap    #9
        bccs    1$
```

```
        jmp     cerror
1$:
        clrl    d0
        rts
```

Nach dem Anlegen obiger Dateien bauen Sie sie mit Hilfe von

```
$ as seteuid.s
$ as setegid.s
```

zusammen, was die Dateien `seteuid.o` und `setegid.o` anlegt.

Dann müssen Sie diese zur LIBSM-Zeile im DNIX-Abschnitt des Samba-Makefiles hinzufügen. Ihre LIBSM-Zeile wird dann ungefähr so aussehen:

```
LIBSM = setegid.o seteuid.o -ln
```

Sie sollten dann die Zeile

```
#define NO_EID
```

aus dem DNIX-Abschnitt von `includes.h` entfernen.

36.4 Red Hat Linux

Standardmäßig fügen manche Versionen von Red Hat Linux bei der Installation folgenden Eintrag zu `/etc/hosts` hinzu:

```
127.0.0.1 loopback "hostname"."domainname"
```

Dies veranlasst Samba, auf das Loopback-Interface zurückzu„*loopen*“. Das Ergebnis ist, dass Samba nicht mehr korrekt kommuniziert und dadurch daran scheitern kann, den Master-Browser und den Verwalter der Master-Browse-Liste zu bestimmen.

Korrektur-Maßnahme: Löschen Sie den Eintrag nach dem Wort „*loopback*“ in der Zeile, die mit 127.0.0.1 beginnt.

36.5 AIX

36.5.1 Sequenzieller Read Ahead

Das Deaktivieren von „*Sequential Read Ahead*“ mit `vmtune -r 0` steigert die Performance von Samba deutlich.

36.6 Solaris

36.6.1 Verbesserungen beim Locking

Manche haben Probleme mit F_SETLKW64/fcntl erlebt, wenn sie Samba unter Solaris betrieben haben. Der eingebaute Dateisperrmechanismus war nicht skalierbar. Die Performance ging runter bis zum dem Punkt, an dem Prozesse beim Versuch, eine Datei zu sperren, in Loops gerieten. Der Prozess versuchte zu sperren, scheiterte und versuchte es wieder. Der Sperrversuch scheiterte, bevor die Sperre erlaubt wurde. Die sichtbare Manifestation dessen waren ein paar Prozesse, die die CPU in Beschlag nahmen, und wenn diese eingebunden wurden, blieben sie stecken, wenn F_SETLKW64 loopte.

Sun hat Patches für Solaris 2.6, 8 und 9 veröffentlicht. Der Patch für Solaris 7 wurde noch nicht veröffentlicht.

Die Patch-Revision für 2.6 ist 105181-34, für 8 ist sie 108528-19 und für 9 ist sie 112233-04.

Nach der Installation dieser Patches ist es zu empfehlen, Samba zu rekonfigurieren und zu rekompilieren.

Wir danken Joe Meslovich für den Hinweis auf diese Patches.

36.6.2 Winbind auf Solaris 9

Nsswitch in Solaris 9 verweigert die Benutzung des Winbind-NSS-Moduls. Dieses Verhalten wurde von Sun im Patch 113476-05 bereinigt. Dieser Patch ist jedoch, da er vom März 2003 stammt, in keinen Roll-up-Paketen enthalten.

Kapitel 37

SAMBA UND ANDERE CIFS-CLIENTS

Dieses Kapitel enthält clientspezifische Informationen.

37.1 Macintosh-Clients

Ja, Thursby <http://www.thursby.com/> hat einen CIFS-Client/Server namens DAVE. <http://www.thursby.com/products/dave.html> Er wird gegen Windows 95, Windows NT /200x/XP und Samba auf Kompatibilität geprüft. Bei Verfassen dieses Textes war DAVE in Version 4.1 erhältlich. Bitte konsultieren Sie Thursbys Webseite für mehr Informationen zu diesem Produkt.

Alternativen — Es gibt zwei freie Implementationen von Appletalk für einige Arten von UNIX-Maschinen und noch einige kommerzielle mehr. Diese Produkte erlauben es Ihnen, native Datei- und Druck-Dienste für Macintosh-Benutzer anzubieten, ohne dass weitere Unterstützung dafür auf dem Macintosh erforderlich wäre. Die zwei freien Implementationen sind Netatalk <http://www.umich.edu/~rsug/netatalk/> und CAP. <http://www.cs.mu.oz.au/appletalk/atalk.html> Diese Packages bieten Macs das, was Samba Benutzern von MS Windows bietet. Für mehr Informationen zu diesen Packages, Samba und Linux (sowie anderen UNIX-basierenden Systemen) sehen Sie sich bitte <http://www.eats.com/linux_mac_win.html> an.

Neuere Versionen des Macintosh (Mac OS X) enthalten Samba.

37.2 OS/2-Clients

37.2.1 Das Konfigurieren von OS/2 Warp Connect oder OS/2 Warp 4

Grundlegend brauchen Sie drei Komponenten:

- Den Datei- und Druck-Client (IBM Peer)
- TCP/IP (Internet-Support)
- Den „*NetBIOS über TCP/IP*“-Treiber (TCPBEUI)

Wie Sie die ersten beiden gemeinsam mit dem Basis-Betriebssystem auf einem leeren System installieren, ist im Warp-Handbuch beschrieben. Wenn Warp bereits installiert wurde, Sie aber nun die Netzwerk-Unterstützung installieren wollen, verwenden Sie den Eintrag „*Selective Install for Networking*“ im Ordner „*System Setup*“.

Das Hinzufügen des „*NetBIOS über TCP/IP*“-Treibers wird nicht im Handbuch beschrieben und auch von der Online-Dokumentation nur gestreift. Starten Sie **MPTS.EXE**, klicken Sie auf **OK**, dann auf **Configure LAPS** und auf **IBM OS/2 NETBIOS OVER TCP/IP** unter **Protocols**. Diese Zeile wird dann in die **Current Configuration** verschoben. Wählen Sie diese Zeile aus, klicken Sie auf **Change number**, und erhöhen Sie den Wert von 0 auf 1. Speichern Sie diese Konfiguration.

Wenn der Samba-Server nicht in Ihrem lokalen Subnetz ist, können Sie optional IP-Namen und -Adressen dieser Server zur **Names List** hinzufügen oder einen WINS-Server (NetBIOS Nameserver, in der Terminologie von IBM und RFC) spezifizieren. Für Warp Connect brauchen Sie eventuell ein Update für den `IBM Peer`, um ihn auf dasselbe Level wie Warp 4 zu bringen. Sehen Sie dazu auf der oben genannten Webseite nach.

37.2.2 Andere Versionen von OS/2 konfigurieren

Dieser Abschnitt behandelt die Konfiguration von OS/2 Warp 3 (nicht Connect), OS/2 1.2, 1.3 oder 2.x.

Sie können den freien Microsoft LAN Manager 2.2c Client für OS/2 verwenden, der unter ftp://ftp.microsoft.com/BusSys/Clients/LANMAN.OS2/ <`ftp://ftp.microsoft.com/BusSys/Clients/LANMAN.OS2/`> erhältlich ist. Kurz gesagt: Editieren Sie die Datei `\OS2VER` im root-Verzeichnis der OS/2-Boot-Partition, und fügen Sie die Zeilen

```
20=setup.exe
20=netwksta.sys
20=netvdd.sys
```

ein, bevor Sie den Client installieren. Verwenden Sie den NICHT den vorhandenen NE2000-Treiber, da er fehlerhaft ist. Probieren Sie stattdessen den NE2000- oder NS2000-Treiber von ftp://ftp.cdrom.com/pub/os2/network/ndis/ <`ftp://ftp.cdrom.com/pub/os2/network/ndis/`> aus.

37.2.3 Druckertreiber-Download für OS/2-Clients

Legen Sie eine Freigabe namens *`[PRINTDRV]`* an, die world-readable ist. Kopieren Sie Ihre OS/2-Treiber-Dateien dorthin. Die `.EA_`-Dateien müssen jedoch weiter separat beleiben, also werden Sie die originalen Installationsdateien benutzen müssen und dürfen keinen installierten Treiber von einem OS/2-System kopieren.

Installieren Sie zuerst den NT-Treiber für diesen Drucker. Dann fügen Sie den Parameter os2 driver map = filename zu Ihrer Datei `smb.conf` hinzu. Als Nächstes weisen Sie in der Datei, die durch *`filename`* bezeichnet wird, den NT-Treibernamen dem OS/2-Treibernamen wie folgt zu:

nt driver name = os2 driver name.device name, e.g.

HP LaserJet 5L = LASERJET.HP LaserJet 5L

Sie können in dieser Datei mehrere Treiberzuweisungen vornehmen.

Wenn Sie nur den OS/2-Treibernamen angeben, aber nicht den Device-Namen, werden im ersten Versuch zwar die Dateien geladen, aber der OS/2-Client wird melden, dass der Treiber nicht verfügbar ist. Im zweiten Anlauf wird es funktionieren. Dies kann durch einfaches Hinzufügen des Device-Namens behoben werden, wonach es schon beim ersten Versuch funktioniert.

37.3 Windows for Workgroups

37.3.1 Neuester TCP/IP-Stack von Microsoft

Verwenden Sie den neuesten TCP/IP-Stack von Microsoft, wenn Sie Windows for Workgroups einsetzen. Die frühen TCP/IP-Stacks hatten viele Bugs.

Microsoft hat ein inkrementelles Upgrade für seine TCP/IP-32-Bit-VxD-Treiber veröffentlicht. Die letzte Release kann auf der FTP-Site ftp.microsoft.com in `/peropsys/windows/public/tcpip/wfwt32.exe` gefunden werden. Es gibt dort auch eine Datei update.txt, die die gelösten Probleme beschreibt. Neue Dateien sind: `WINSOCK.DLL`, `TELNET.EXE`, `WSOCK.386`, `VNBT.386`, `WSTCP.386`, `TRACERT.EXE`, `NETSTAT.EXE` und `NBTSTAT.EXE`.

37.3.2 Das Löschen von .pwl-Dateien nach Passwort-Änderungen

Windows for Workgroups arbeitet lausig, wenn es um Passwörter geht. Wenn Sie Passwörter auf entweder der UNIX-Mascine oder dem PC ändern, ist es am sichersten, die .pwl-Dateien im Windows-Verzeichnis zu löschen. Der PC wird sich darüber beschweren, diese Dateien nicht zu finden, sich aber bald damit abfinden und Ihnen erlauben, das neue Passwort einzugeben.

Wenn Sie dies nicht tun, kann es sein, dass Windows for Workgroups sich an das alte Passwort erinnert und es verwendet, auch wenn Sie ein neues angegeben haben.

Oft wird Windows for Workgroups ein Passwort gänzlich ignorieren, das Sie in einer Dialog-Box angeben.

37.3.3 Den Umgang mit Passwörtern in Windows for Workgroups konfigurieren

Auf der letzten Diskette (Diskette 8) des WFW-3.11-Diskettensatzes gibt es ein Programm namens `admincfg.exe`. Um es zu installieren, geben Sie `EXPAND A:\ADMINCFG.EX_ C:\WINDOWS\ADMINCFG.EXE` ein. Fügen Sie dann über das Menü **New** im Program Manager ein Icon hinzu. Dieses Programm erlaubt Ihnen die Kontrolle darüber, wie WFW mit Passwörtern umgeht, z.B. beim Ausschalten von Passwort-Caching und so weiter.

37.3.4 Groß-/Kleinschreibung in Passwörtern

Windows for Workgroups setzt das ganze Passwort in Großbuchstaben, bevor es es an den Server sendet. UNIX-Passwörter können jedoch zwischen Groß-/Kleinschreibung unterscheiden. Prüfen Sie die Informationen zum Parameter password level in der `smb.conf`, um angeben zu können, ob Samba bei der Prüfung des Passworts die Großschreibung versuchen soll.

37.3.5 TCP/IP als Standard-Protokoll verwenden

Um Reports über Drucker-Queues zu unterstützen, werden Sie unter Umständen unter WfW TCP/IP als Standard-Protokoll verwenden müssen. Aus irgendeinem Grund kann das Belassen von NetBEUI als Standardeinstellung dazu führen, dass die Queue-Reports auf manchen Systemen nicht funktionieren. Dies ist möglicherweise ein Bug in WfW.

37.3.6 Geschwindigkeitssteigerung

Einige Anwender haben festgestellt, dass sie eine große Beschleunigung erzielen, wenn sie den Parameter *DefaultRcvWindow* im Abschnitt *[MSTCP]* der Datei `SYSTEM.INI` unter WfW auf den Wert 3072 setzen.

Meine eigene Erfahrung mit *DefaultRcvWindow* ist, dass ich eine viel bessere Performance mit großen Werten (16384 oder höher) erziele. Andere berichten, dass alles über 3072 wieder enorm bremst. Jemand hat sogar einen Geschwindigkeitsabfall auf 1/30 gemessen, als er den Wert von 3072 auf 8192 erhöht hat.

37.4 Windows 95/98

Bei der Verwendung von Windows 95 OEM SR2 werden folgende Updates empfohlen, wenn Samba eingesetzt wird. Bitte beachten Sie, dass die oben genannte Änderung Sie betreffen wird, sobald diese Updates installiert worden sind.

Es gibt mehr Updates als die hier erwähnten. Wir verweisen Sie auf die Microsoft-Website für die verfügbaren Updates zu Ihrer spezifischen Version von Windows 95.

Kernel-Update: KRNLUPD.EXE
Ping-Fix: PINGUPD.EXE
RPC-Update: RPCRTUPD.EXE
TCP/IP-Update: VIPUPD.EXE
Redirector-Update: VRDRUPD.EXE

Auch bei Verwendung von MS Outlook ist es wünschenswert, den Fix von **OLEUPD.EXE** zu installieren. Dieser Fix kann das Hängenbleiben beim Beenden von Outlook verhindern, und Sie könnten eine deutliche Beschleunigung bemerken, wenn Sie auf die Netzwerkumgebung zugreifen.

37.4.1 Geschwindigkeitssteigerung

Konfigurieren Sie die Windows 95-TCP/IP-Registrierungseinträge, um eine bessere Performance zu erreichen. Ich verwende ein Programm namens **MTUSPEED.exe** aus dem Internet. Es gibt verschiedene andere Utilities dieser Art, die frei verfügbar sind.

37.5 Windows 2000 Service Pack 2

Es gibt einige lästige Dinge an Windows 2000 SP2. Eines davon tritt nur auf, wenn man einen Samba-Server verwendet, um Benutzer-Profile für Windows 2000 SP2-Clients in einer Windows-Domäne bereitzustellen. Dies geht davon aus, dass Samba Domänen-Mitglied ist, aber das Problem wird meist dann auftreten, wenn Samba es nicht ist.

Um Profile erfolgreich für Windows 2000 SP2-Clients anzubieten (ohne PDC zu sein), muss Samba den Parameter nt acl support = no für die Freigabe gesetzt haben, die die Roaming-Profile beinhaltet. Wenn dies nicht erfolgt, wird sich der Windows 2000 SP2-Client darüber beschweren, dass er nicht imstande ist, auf das Profil zuzugreifen (Access Denied) und mehrfach Kopien davon auf der Platte anlegen (DOMAIN.user.001, DOMAIN.user.002 und so weiter). Lesen Sie in der Manpage zu `smb.conf` mehr über diesen Parameter. Beachten Sie auch, dass der Parameter nt acl support in Releases vor Samba 2.2.2 formal ein globaler Parameter war.

Beispiel **??** zeigt eine minimale Profil-Freigabe.

Beispiel 37.5.1. Minimale Profil-Freigabe

```
[profile]
       path = /export/profile
       create mask = 0600
       directory mask = 0700
       nt acl support = no
       read only = no
```

Der Grund für diesen Bug ist, dass der Windows 2000 SP2-Client den Security-Deskriptor für das Profil, das die SID des Samba-Servers enthält, kopiert und nicht die Domänen-SID. Der Client vergleicht die SID für SAMBA\user und stellt fest, dass sie von der SID für DOMAIN\user abweicht. Daher kommt es zu der Meldung access denied.

Durch Deaktivieren des Parameters nt acl support sendet Samba dem Windows 200x-Client eine Antwort auf den Aufruf „*QuerySecurityDescriptor trans2*“, die den Client dazu veranlasst, eine Standard-ACL für das Profil zu setzen. Diese Standard-ACL enthält:

*DOMAIN**user* „Full Control“>

Anmerkung

Dieser Bug tritt nicht auf, wenn man Winbind zum Anlegen von Benutzerkonten für Domänen-Benutzer auf dem Samba-Host verwendet.

37.6 Windows NT 3.1

Wenn Sie Probleme mit der Kommunikation über Router mit Windows NT 3.1-Workstations haben, lesen Sie den Microsoft Knowledge-Base-Artikel. <`http://support.microsoft.com/default.aspx?scid=kb;Q103765`>

Kapitel 38

PERFORMANCE-TUNING FÜR SAMBA

38.1 Vergleiche

Der Samba-Server verwendet TCP zur Kommunikation mit dem Client. Um die wirkliche Performance beurteilen zu können, sollte sie mit der anderer Programme verglichen werden, die ebenfalls TCP verwenden. Die am leichtesten verfügbaren Programme dieser Art sind ftp oder andere auf TCP basierende SMB-Server.

Um Samba mit anderen Servern wie Windows-NT- oder Windows-for-Workgroups-Servern vergleichen zu können, müssen alle Protokolle außer TCP entweder auf dem Client oder auf dem Server deaktiviert werden. Ansonsten besteht die Möglichkeit, unwissentlich ein gänzlich anderes Protokoll (wie NetBEUI) zu verwenden. Die resultierenden Ergebnisse wären unbrauchbar.

Allgemein kann gesagt werden, dass Samba ähnliche Durchsatzraten wie ftp erzielt. Es sollte ein deutliches Stück schneller als NFS arbeiten, wobei dies vom System abhängt.

Es gibt einige Vergleiche zwischen Samba und Novell, NFS oder NT. In manchen schneidet Samba am besten ab, in anderen am schlechtesten. Es ist zu vermuten, dass der größte beeinflussende Faktor nicht Samba selbst, sondern die Kombination von Hardware und Treibern der verschiedenen Systeme ist. Bei der Verwendung ähnlicher Hardware sollte Samba sehr wohl wettbewerbsfähig sein.

38.2 Socket-Optionen

Es gibt einige Socket-Optionen, die die Performance eines TCP-basierten Servers wie Samba stark beeinflussen können.

Die von Samba verwendeten Socket-Optionen können sowohl mit der Option `-O` auf der Befehlszeile gesetzt werden als auch in der Datei `smb.conf`.

Der Abschnitt zu socket options in der Manpage zu `smb.conf` beschreibt deren Verwendung und gibt diesbezügliche Empfehlungen.

Die Socket-Optionen richtig zu setzen kann einen großen Einfluss auf die Performance haben; sind sie jedoch falsch gesetzt, kann dies die Performance ebenso sehr verschlechtern. Die korrekten Parameter sind in hohem Maße vom lokalen Netzwerk abhängig.

Die Socket-Option TCP_NODELAY ist diejenige, die den größten Leistungsunterschied für die meisten Netzwerke auszumachen scheint. Viele Anwender berichten, dass das Hinzufügen von
socket options = TCP_NODELAY die Lese-Performance eines Samba-Laufwerks verdoppelt. Die beste Erklärung hierfür scheint, dass der Microsoft TCP/IP-Stack sehr langsam beim Senden von TCP-ACKs ist.

Es wurde berichtet, dass das Setzen von *socket options = SO_RCVBUF=8192* in smb.conf die Samba-Performance auf dem Loopback-Interface (IP 127.0.0.1) stark verschlechtert. Es wird daher empfohlen, vor dem Setzen jeglicher *socket options* die Auswirkungen quantitativ auf dem zu konfigurierenden Server zu messen.

38.3 Read Size

Die Option read size beeinflusst die Überschneidungen von Platten-Schreib/Lese-Vorgängen mit Netzwerk-Schreib/Lese-Vorgängen. Wenn die von einigen SMB-Befehlen (momentan SMBwrite, SMBwriteX und SMBreadbraw) transferierte Datenmenge über diesem Wert liegt, beginnt der Server bereits Daten zu schreiben, bevor er noch das ganze TCP-Paket vom Netzwerk empfangen hat. Im Falle von SMBreadbraw beginnt er Daten an das Netz zu senden, bevor er noch alle Daten von der Platte gelesen hat.

Diese Überschneidung funktioniert am besten, wenn die Platten- und Netzwerk-Zugriffsgeschwindigkeit ungefähr gleich sind. Bei großen Unterschieden zwischen diesen beiden Werten hat dieser Parameter wenig Auswirkung.

Der Standard-Wert ist 16384, jedoch wurde bisher wenig experimentiert, um den optimalen Wert zu finden, es ist außerdem anzunehmen, dass dieser Wert stark zwischen einzelnen Systemen variiert. Ein Wert über 65536 ist nutzlos und verursacht nur unnötig hohe Speicherbelegung.

38.4 Max Xmit

Beim Verbindungsaufbau verhandeln Client und Server einen Wert namens *maximum transmit* size, der die Größe nahzu aller SMB-Befehle beschränkt. Der Startwert für diese Verhandlung kann mit der Option max xmit in `smb.conf` gesetzt werden. Beachten Sie, dass dies die maximale Größe der SMB-Anfragen ist, die Samba akzeptiert, jedoch nicht die maximale Größe, die der Client akzeptiert. Der Client legt die von ihm akzeptierte maximale SMB-Anfragen-Größe fest, und Samba berücksichtigt dieses Limit.

Dieser Wert beträgt standardmäßig 65536 Bytes (das Maximum), aber es ist möglich, dass manche Clients mit einer kleineren Übertragungseinheit schneller arbeiten. Werte unter 2048 verursachen meist ernsthafte Probleme. Im Normalfall ist der Standard-Wert der beste.

38.5 Log-Level

Wird der Log-Level (auch als debug level bekannt) auf Werte größer als 2 gesetzt, resultiert dies meist in einem starken Performance-Einbruch. Dies liegt daran, dass der Server nach jeder Operation das Logfile „*flusht*“.

38.6 Read Raw

Die read raw-Operation ist eine optimierte Lese-Operation mit geringer Latenz-Zeit. Ein Server kann diese wahlweise unterstützen, Samba trägt dem dadurch Rechnung, dass die Unterstützung für read raw optional ist, wobei diese standardmäßig aktiv ist.

In einigen Fällen können Clients mit dem Parameter read raw nicht besonders gut umgehen. Dann hat seine Verwendung eine schlechtere Performance zur Folge als die Verwendung der konventionellen Lese-Operation.

Es liegt nahe, die Option read raw = no auszuprobieren und die Auswirkungen im jeweiligen Netzwerk zu prüfen. Diese Einstellung kann die Performance steigern, verringern oder auch gar nicht beeinflussen. Nur ein Test kann dies wirklich zeigen.

38.7 Write Raw

Die write raw-Operation ist eine optimierte Schreiboperation mit geringer Latenz-Zeit. Ein Server kann diese wahlweise unterstützen; Samba trägt dem dadurch Rechnung, dass die Unterstützung für write raw optional ist, wobei diese standardmäßig aktiv ist.

Einige Maschinen arbeiten mit write raw langsamer als mit normalem Schreiben. In diesem Fall erscheint es besser, diese Option zu ändern.

38.8 Slow Logins

„*Slow Logins*“ hängen so gut wie immer mit der Zeit zusammen, die benötigt wird, um das Passwort zu überprüfen. Das Verwenden des niedrigstmöglichen password level wird dies verbessern.

38.9 Client-Tuning

Oft kann ein Geschwindigkeitsproblem auf den Client zurückgeführt werden. Der Client (z.B. Windows for Workgroups) kann oft noch auf bessere TCP-Performance getunt werden. Lesen Sie diesbezüglich die jeweiligen Abschnitte in Kapitel **??** „Samba und andere CIFS-Clients“.

38.10 Samba-Performance-Problem nach dem Wechsel des Linux-Kernels

Ein Samba-Anwender hat das Folgende an die Samba-Mailingliste geschrieben:

Ich verwende auf meinem Server Gentoo Linux und Samba 2.2.8a. Unlängst habe ich meinen Kernel von `linux-2.4.19-gentoo-r10` auf `linux-2.4.20-wolk4.0s` geändert. Nun habe ich ein Performance-Problem mit Samba. Viele von euch werden vielleicht sagen, „*Versuche es mit den ursprünglichen Kernel-Sourcen!*“. Tja, ich habe das versucht, und es hat nicht funktioniert. Ich habe ein 100-MBit-LAN und zwei Rechner (Linux und Windows 2000). Der Linux-Server gibt Verzeichnisse mit DivX-Dateien frei, der Windows-Client spielt diese über das LAN ab. Zuvor, als ich noch den 2.4.19-Kernel verwendet habe, lief alles sauber, aber nun stocken und stoppen die Filme. Der Versuch, die Dateien vom Server auf den Windows-Rechner zu schieben, zeigte, dass dies schrecklich langsam ist.

Die Antwort, die er erhalten hat, war diese:

Besorge dir das mii-Tool und überprüfe die Duplex-Einstellungen auf deiner Netzwerkkarte. Meine Vermutung ist, dass dies ein Problem in der Verbindungsschicht ist, keines in der Anwendungsschicht. Überprüfe außerdem, ob die Ausgaben von ifconfig in Hinblick auf Kollisionen usw. normal für Ethernet erscheinen.

38.11 Beschäigte tdb-Dateien

Unser Samba-PDC-Server verwaltet seit drei Jahren ohne Probleme 3 Tbyte Daten für unsere mehr als 500 Benutzer [Windows NT/XP]. Heute wurden alle Freigaben plötzlich sehr langsam. Außerdem begann der Haupt-smbd-Prozess damit, neue Sub-smbd-Prozesse zu starten, so dass wir schließlich über 1600 laufende smbd-Prozesse hatten (normalerweise haben wir durchschnittlich 250). Dies brachte den SUN E3500-Cluster zweimal zum Absturz. Nach vielem Suchen habe ich entschieden, **rm /var/locks/*.tdb** auszuführen. Endlich bin ich wieder glücklich!

Frage: Gibt es eine Methode, um die tdb-Dateien in gutem Zustand zu halten? Wie kann ich frühzeitig feststellen, dass diese Dateien beschädigt sind?

Antwort: Führe **tdbbackup** nach jedem Stopp und vor jedem Start von nmbd aus. (Anmerkung des Übersetzers: Eine Möglichkeit ist, dies in das rcsmb/rcnmb-Skript aufzunehmen, das viele Distributionen verwenden.)

Frage: Was ich noch bemerken möchte, ist, dass die Antwortzeiten der Dienste bei weitem niedriger erscheinen als vor dem Bereinigen der Sperrdateien. Gibt es Möglichkeiten, diese im Top-Zustand zu halten?

Antwort: Ja. Selbe Antwort wie zuvor!

38.12 Samba-Performance ist sehr langsam

Der Administrator einer Site hat über sehr verblüffende Symptome berichtet, die mit MYOB Premier zusammenhängen, das seine Datendateien öffnet und darauf zugreift. Einige Operationen würden zwischen 40 und 45 Sekunden dauern.

Es stellte sich heraus, dass das Drucker-Überwachungsprogramm, das auf den Windows-Clients läuft, das Problem verursacht hat. Aus den Log-Dateien wurde dessen Aktivität im 1-Sekunden-Takt ersichtlich.

Das Stoppen dieses Überwachungsprogramms ergab Netzwerkzugriffe in normaler (schneller) Geschwindigkeit. Das Neustarten des Programmes ließ die Geschwindigkeit wieder stark abfallen. Der Drucker war ein Canon lbp810, und der betreffende Task hieß so ähnlich wie CAPON (exakte Schreibweise unbekannt). Die Überwachungssoftware zeigte einen „*Druck wird ausgeführt*“-Dialog auf dem Windows-Client.

Wir haben dies festgestellt, indem wir eine frische Windows-Installation verwendeten und die Anwendung bei jedem Installationsschritt einer anderen Software ausprobiert haben (wir mussten dies oft tun ...).

Und die Moral von der Geschicht': Überprüfe alles (andere Software eingeschlossen)!

Kapitel 39

DNS UND DHCP: KONFIGURATIONSANLEITUNG

39.1 Eigenschaften und Vorzüge

Es gibt wenige Themen in der UNIX-Welt, die zu solchen Auseinandersetzungen führen wie das Domain Name System (DNS) und das Dynamic Host Configuration Protocol (DHCP). Nicht alle Argumente, die für oder gegen einzelne Implementationen von DNS und DHCP angeführt werden, sind stichhaltig.

Wir leben in einem modernen Zeitalter, in dem viele Anwender von Informationstechnologie Mobilität und Freiheit anstreben. Besonders Nutzer von MS Windows erwarten, ihr Notebook einfach an eine Netzwerk-Buchse anschließen zu können und dass die Dinge „*einfach funktionieren*".

UNIX-Administratoren haben ein gutes Argument. Vieles aus der normativen Praxis in der MS Windows-Welt grenzt unter Sicherheitsgesichtspunkten im besten Fall an schlechte Gewohnheiten. MS Windows Netzwerk-Protokolle erlauben es Workstations, sich willkürlich an einem Netzwerk anzumelden. Windows 2000 Active Directory registriert Einträge im DNS-Namensraum, die UNIX-Administratoren nur so erstaunen. Willkommen in der neuen Welt!

Der Zweck dieses Kapitels ist, die Konfiguration von Internet Software Consortium-(ISC-) DNS- und DHCP-Servern zu demonstrieren, um dynamische Dienste anzubieten, die kompatibel mit ihren Entsprechungen in den Microsoft Windows 2000 Server-Produkten sind.

Der Zweck dieses Kapitels ist lediglich, ein funktionierendes Beispiel für Konfigurationsdateien anzubieten, und zwar sowohl für DNS- als auch für DHCP-Server. Die verwendeten Beispiele passen zu Konfigurationsbeispielen, die in anderen Bereichen dieses Dokuments angeführt werden.

Dieses Kapitel stellt ausdrücklich kein Tutorial dar, und es soll auch keine Referenz zu DNS und DHCP sein, da dies weit über den Horizont und die Zielsetzung dieses Dokuments hinausginge. Jeder, der detailliertere Materialien zu DNS oder DHCP braucht, sollte die ISC-Website auf <`http://www.isc.org`> besuchen. Jene, die eher gedruckten Text bevorzugen, könnten Interesse an den O'Reilly-Publikationen zu diesen Themen finden.

39.2 Beispielkonfiguration

Das Domain Name System ist für das Internet, was das Wasser für das Leben ist. Durch dieses System werden fast alle Informationsressourcen (Host-Namen) in ihre Internet-Protokoll-(IP-)Adressen aufgelöst. Die Windows-Netzwerk-Technologie versucht sehr stark, die Komplexitäten von DNS zu vermeiden, aber leider hat DNS gewonnen. Die Alternative zu DNS, Windows Internet Name Service (WINS), ein Artefakt aus der Zeit, in der NetBIOS-Netzwerke über TCP/IP-Protokoll betrieben wurden, hat nicht nur Skalierungsprobleme, sondern auch einen flachen, nicht-hierarchischen Namensraum, der unverwaltbar wurde, als die Größe und Komplexität der Informationstechnologie-Netzwerke wuchs.

WINS ist eine Microsoft-Implementation des NetBIOS Name Service (NBNS) laut RFC1001/1002. Es erlaubt NetBIOS-Clients (wie Microsoft Windows-Maschinen), einen willkürlichen Maschinen-Namen, den der Administrator oder Benutzer gewählt hat, gemeinsam mit der zugewiesenen IP-Adresse zu registrieren. Durch die Verwendung von WINS können Netzwerk-Client-Maschinen Maschinen-Namen in ihre IP-Adressen auflösen.

Der Bedarf nach einer Alternative zu den Beschränkungen des NetBIOS-Netzwerks führte Microsoft schließlich dazu, DNS und Active Directory zu verwenden. Die neue Implementation von Microsoft versucht, DNS in einer ähnlichen Weise zu verwenden, wie WINS für NetBIOS verwendet wird. Sowohl WINS als auch Microsoft DNS basieren auf dem dynamischen Registrieren von Namen.

MS Windows-Clients können beim Start eine dynamische Namensregistrierung am DNS-Server durchführen. Alternativ ist es dort, wo DHCP zur Zuweisung der IP-Adressen verwendet wird, möglich, Hostnamen und deren IP-Adressen durch den DHCP-Server zu registrieren, sobald der Client ein so genanntes IP-Lease akzeptiert. Zuletzt kann MS DNS Hostnamen via MS WINS auflösen.

Die folgenden Konfigurationen zeigen einen einfachen Dynamic-DNS-Server und einen einfachen DHCP-Server, der zu der DNS-Konfiguration passt.

39.2.1 Dynamisches DNS

Die Beispiel-DNS-Konfiguration erfolgt für ein privates Netzwerk im IP-Adressraum 192.168.1.0/24. Der „*private class*“-Netzwerk-Adressraum ist in RFC1918 festgelegt.

Es wird angenommen, dass dieses Netzwerk hinter einer sicheren Firewall liegen wird. Die folgenden Dateien arbeiten mit ISC BIND Version 9. BIND ist der Berkeley Internet Name Daemon. Die folgenden Konfigurationsdateien werden angeboten:

Die Hauptkonfigurationsdatei `/etc/named.conf` bestimmt die Lage aller weiteren Konfigurationsdateien. Die Lage und der Name dieser Datei wird im Start-Skript des Betriebssystems festgelegt.

```
# Quenya.Org configuration file

acl mynet {
   192.168.1.0/24;
   127.0.0.1;
```

```
};

options {

   directory "/var/named";
   listen-on-v6 { any; };
   notify no;
   forward first;
   forwarders {
      192.168.1.1;
      };
   auth-nxdomain yes;
   multiple-cnames yes;
   listen-on {
      mynet;
      };
};

# The following three zone definitions do not need any modification.
# The first one defines localhost while the second defines the
# reverse lookup for localhost. The last zone "." is the
# definition of the root name servers.

zone "localhost" in {
   type master;
   file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
   type master;
   file "127.0.0.zone";
};

zone "." in {
   type hint;
   file "root.hint";
};

# You can insert further zone records for your own domains below.

zone "quenya.org" {
   type master;
   file "/var/named/quenya.org.hosts";
   allow-query {
      mynet;
      };
   allow-transfer {
      mynet;
```

```
      };
   allow-update {
      mynet;
      };
   };

zone "1.168.192.in-addr.arpa" {
   type master;
   file "/var/named/192.168.1.0.rev";
   allow-query {
      mynet;
   };
   allow-transfer {
      mynet;
   };
   allow-update {
      mynet;
   };
};
```

Die folgenden Dateien liegen alle im Verzeichnis `/var/named`. Dies ist die Datei `/var/named/localhost.zone`:

```
$TTL 1W
@               IN SOA  @   root (
            42              ; serial (d. adams)
            2D              ; refresh
            4H              ; retry
            6W              ; expiry
            1W )            ; minimum

      IN NS           @
      IN A            127.0.0.1
```

Die Datei `/var/named/127.0.0.zone` sieht wie folgt aus:

```
$TTL 1W
@               IN SOA          localhost.  root.localhost. (
            42              ; serial (d. adams)
            2D              ; refresh
            4H              ; retry
            6W              ; expiry
            1W )            ; minimum

            IN NS           localhost.
1               IN PTR          localhost.
```

Die Datei /var/named/quenya.org.host sieht so aus:

```
$ORIGIN .
$TTL 38400      ; 10 hours 40 minutes
quenya.org      IN SOA  marvel.quenya.org. root.quenya.org. (
            2003021832 ; serial
            10800      ; refresh (3 hours)
            3600       ; retry (1 hour)
            604800     ; expire (1 week)
            38400      ; minimum (10 hours 40 minutes)
            )
         NS      marvel.quenya.org.
         MX      10 mail.quenya.org.
$ORIGIN quenya.org.
frodo                   A       192.168.1.1
marvel                  A       192.168.1.2
;
mail                    CNAME   marvel
www                     CNAME   marvel
```

Die Datei /var/named/192.168.1.0.rev sieht so aus:

```
$ORIGIN .
$TTL 38400      ; 10 hours 40 minutes
1.168.192.in-addr.arpa  IN SOA  marvel.quenya.org. root.quenya.org. (
            2003021824 ; serial
            10800      ; refresh (3 hours)
            3600       ; retry (1 hour)
            604800     ; expire (1 week)
            38400      ; minimum (10 hours 40 minutes)
            )
         NS      marvel.quenya.org.
$ORIGIN 1.168.192.in-addr.arpa.
1                       PTR     frodo.quenya.org.
2                       PTR     marvel.quenya.org.
```

Die oben gezeigten Dateien wurden von einem vollständig funktionierenden System kopiert. Alle dynamisch registrierten Einträge wurden entfernt. Zusätzlich zu diesen Dateien wird BIND Version 9 für jede der dynamischen Registrationsdateien eine Datei anlegen, die die Endung `.jnl` hat. Machen Sie sich nicht an diesen Dateien zu schaffen, auch nicht an den `.jnl`-Dateien!

39.2.2 DHCP-Server

Folgende Datei wird mit dem ISC DHCP Server Version 3 verwendet. Die Datei liegt in `/etc/dhcpd.conf`:

```
ddns-updates on;
ddns-domainname "quenya.org";
option ntp-servers 192.168.1.2;
ddns-update-style ad-hoc;
allow unknown-clients;
default-lease-time 86400;
max-lease-time 172800;

option domain-name "quenya.org";
option domain-name-servers 192.168.1.2;
option netbios-name-servers 192.168.1.2;
option netbios-dd-server 192.168.1.2;
option netbios-node-type 8;

subnet 192.168.1.0 netmask 255.255.255.0 {
   range dynamic-bootp 192.168.1.60 192.168.1.254;
   option subnet-mask 255.255.255.0;
   option routers 192.168.1.2;
   allow unknown-clients;
}
```

Im obigen Beispiel werden IP-Adressen zwischen 192.168.1.1 und 192.168.1.59 für fixe (üblicherweise als `hard-wired` bezeichnete) IP-Adressen reserviert. Die Adressen zwischen 192.168.1.60 und 192.168.1.254 werden zur dynamischen Verwendung bereitgestellt.

Kapitel 40

WEITERE HILFSQUELLEN

40.1 Webseiten

- *CIFS: Common Insecurities Fail Scrutiny* von „*Hobbit*“ <http://hr.uoregon.edu/davidrl/cifs.txt>
- *Doing the Samba on Windows* von Financial Review <http://afr.com/it/2002/10/01/FFXDF43AP6D.html>
- *Implementing CIFS* von Christopher R. Hertel <http://ubiqx.org/cifs/>
- *Just What Is SMB?* von Richard Sharpe <http://samba.anu.edu.au/cifs/docs/what-is-smb.html>
- *Opening Windows Everywhere* von Mike Warfield <http://www.linux-mag.com/1999-05/samba_01.html>
- *SMB HOWTO* von David Wood <http://www.tldp.org/HOWTO/SMB-HOWTO.html>
- *SMB/CIFS by The Root* von „*ledin*“ <http://www.phrack.org/phrack/60/p60-0x0b.txt>
- *The Story of Samba* von Christopher R. Hertel <http://www.linux-mag.com/1999-09/samba_01.html>
- *The Unofficial Samba HOWTO* von David Lechnyr <http://hr.uoregon.edu/davidrl/samba/>
- *Understanding the Network Neighborhood* von Christopher R. Hertel <http://www.linux-mag.com/2001-05/smb_01.html>
- *Using Samba as a PDC* von Andrew Bartlett <http://www.linux-mag.com/2002-02/samba_01.html>
- *PDF version of the Troubleshooting Techniques chapter* aus der zweiten Auflage von „*Sam's Teach Yourself Samba in 24 Hours*“ (erschienen am 12.12.2001) <http://ru.samba.org/samba/ftp/docs/Samba24Hc13.pdf>
- *Slide presentations* von Mitgliedern des Samba-Team <http://ru.samba.org/samba/ftp/slides/>

- *Introduction to Samba-3.0* von Motonobu Takahashi (written in Japanese). <http://www.atmarkit.co.jp/flinux/special/samba3/samba3a.html>
- *Understanding the Network Neighborhood*, vom Samba-Team-Mitglied Chris Hertel. Dieser Artikel erschien im Mai 2001 im Linux Magazine. <http://www.linux-mag.com/2001-05/smb_01.html>
- *Samba 2.0.x Troubleshooting guide* von Paul Green <ftp://ftp.stratus.com/pub/vos/customers/samba/>
- *Ten Years of Samba* <http://samba.org/samba/docs/10years.html>
- *Samba Authenticated Gateway HOWTO* <http://tldp.org/HOWTO/Samba-Authenticated-Gatew
html>
- *An Introduction to Samba* <http://samba.org/samba/docs/SambaIntro.html>
- *What is CIFS?* <http://www.samba.org/cifs/>
- *WFWG: Password Caching and How It Affects LAN Manager Security* in der Microsoft Knowledge Base <http://support.microsoft.com/support/kb/articles/q92/5/88.asp>

40.2 Verwandte Updates von Microsoft

- *Enhanced Encryption for Windows 95 Password Cache* <http://support.microsoft.com/support/kb/articles/q92/5/88.asp>
- *Windows '95 File Sharing Updates* <http://support.microsoft.com/support/kb/articles/q136/4/18.asp>
- *Windows for Workgroups Sharing Updates* <http://support.microsoft.com/support/kb/articles/q136/4/18.asp>

SUBJECT INDEX